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

Presentado a:

JOHN FREDDY QUINTERO –

Director de curso
202337164A_1438

JOHN OSWAAL RATIVA VELANDIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2023

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

JOHN OSWAAL RATIVA VELANDIA

JOHN FREDDY QUINTERO
Director de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2023

RESUMEN

El presente informe técnico es un documento que detalla de manera específica las actividades llevadas a cabo en cumplimiento de los requerimientos establecidos por la empresa WHITEHOUSE SECURITY. El objetivo primordial de este informe es proporcionar una visión más detallada de las acciones realizadas para abordar una situación crítica: el robo de información de los equipos de la compañía.

Para comenzar, se describe en detalle el proceso de identificación de vulnerabilidades en las máquinas que fueron objeto de robo de información. Este proceso involucró el uso de diversas herramientas tecnológicas de código abierto, cada etapa de este proceso se documenta minuciosamente, desde la selección de las herramientas hasta la ejecución de los escaneos y la obtención de resultados.

Además de identificar las vulnerabilidades, este informe también se adentra en la recreación de la intrusión en las máquinas afectadas. Esto implica trazar el camino que los atacantes siguieron para acceder a la información sensible. Se analiza cómo pudo haber sido el ataque, los vectores de entrada utilizados y cualquier táctica o técnica empleada por los intrusos.

La tercera sección del informe se centra en las medidas de contención que se implementaron para detener el ataque y prevenir daños adicionales. Esto puede incluir la desconexión de sistemas comprometidos, la aplicación de parches de seguridad y otras acciones destinadas a asegurar que los atacantes no puedan continuar con sus actividades maliciosas.

Una parte esencial de este informe se dedica a la "hardenización", que se refiere al fortalecimiento de la seguridad de los sistemas para evitar o minimizar futuros ataques. Se detallan las medidas de seguridad recomendadas, como la implementación de firewalls, la actualización constante de software.

Finalmente, el informe concluye con una serie de recomendaciones específicas para prevenir ataques tanto desde la red externa como desde el interior de la organización.

CONTENIDO

Tabla de Figuras

Tabla de Tablas

GLOSARIO

Amenaza Cibernética: Un riesgo potencial para la seguridad de la información, como malware, ataques de phishing o intentos de intrusión.

Análisis Forense: Proceso de investigación de incidentes de seguridad para determinar la causa raíz y el alcance de un ataque.

Anomalía: Un comportamiento inusual o atípico en una red o sistema que podría indicar una amenaza cibernética.

Antivirus: Software diseñado para detectar y eliminar malware en un sistema.

Ataque informático: Un intento malicioso de comprometer la confidencialidad, integridad o disponibilidad de sistemas de información.

Auditoría de Seguridad: Una revisión sistemática y exhaustiva de las medidas de seguridad de un sistema o red para identificar vulnerabilidades y deficiencias.

Ciberataque: Un ataque que está ocurriendo actualmente y que requiere una respuesta inmediata.

Conciencia de Seguridad: La comprensión y el conocimiento de las amenazas de seguridad y las mejores prácticas de seguridad por parte de los usuarios y administradores de sistemas.

Correlación de Eventos: Proceso de identificar patrones y relaciones entre eventos de seguridad para detectar amenazas.

Detección de Amenazas: Identificación de actividades o eventos que indican la presencia de amenazas cibernéticas.

Equipo de respuesta a incidentes de seguridad cibernética (CSIRT): Un equipo especializado encargado de gestionar y responder a incidentes de seguridad cibernética en una organización.

Firewall: Un sistema de seguridad que controla el tráfico de red y protege contra accesos no autorizados.

Fuerza Bruta: Un ataque en el que un atacante intenta adivinar una contraseña probando todas las combinaciones posibles hasta encontrar la correcta.

Gestión de Riesgos: Proceso de identificación, evaluación y mitigación de los riesgos de seguridad en un sistema o red.

Hardening: Proceso de fortalecimiento de la seguridad de un sistema informático o red mediante la aplicación de medidas específicas para reducir las vulnerabilidades y la exposición a amenazas.

Incidente de Seguridad: Un evento que compromete la confidencialidad, integridad o disponibilidad de los datos o sistemas y que puede ser el resultado de un ataque o una falla de seguridad.

Malware: Software malicioso diseñado para dañar, robar información o tomar el control de sistemas informáticos sin el consentimiento del propietario.

Parche de Seguridad: Actualización de software diseñada para corregir vulnerabilidades conocidas y mejorar la seguridad.

Puerto: Un punto de conexión a través del cual las computadoras y los sistemas se comunican en una red, a menudo asociado con un servicio específico (por ejemplo, el puerto 80 para HTTP).

Registros de Seguridad: Información detallada de eventos de seguridad, como registros de sistemas, aplicaciones y redes, que se utilizan en SIEM para el análisis.

SIEM: Plataforma de seguridad que combina la gestión de información de seguridad con la gestión de eventos, permitiendo la correlación y el análisis de datos de seguridad.

Simulación de incidentes: Ejercicio planificado en el que se simula un incidente de seguridad cibernética para entrenar y evaluar la capacidad de respuesta de una organización.

Trazabilidad de Amenazas: Seguimiento y documentación de las actividades y tácticas utilizadas por los atacantes en un entorno de seguridad.

Virus: Software malicioso que se replica y se adjunta a otros programas para propagarse y causar daño.

Vulnerabilidad: Una debilidad o fallo en un sistema o software que puede ser explotado por un atacante para comprometer la seguridad.

INTRODUCCIÓN

Dentro del desarrollo del documento de informe final del ataque generado se toma en cuenta, la interpretación de varios escenarios de consulta como conceptos básicos para equipo de Red Team & Blue Team, y posteriormente se crean máquinas virtuales para el desarrollo de actividades con parámetros mínimos de configuración.

Posteriormente, se realiza una investigación y desarrollo de varios escenarios de conceptos básicos para equipo de Red Team & Blue Team, el desarrollo de escenarios de vulneración de máquinas, identificando cuáles son sus posibles fallas a la seguridad por medio de uso de herramientas especializadas que permita acceder de forma exitosa y que de este modo se identifiquen los puntos a mejorar.

Por último, el desarrollo de escenarios de estrategias de contención mediante el análisis de riesgos y vulnerabilidades, que permitan mejorar la seguridad de las máquinas afectadas.

OBJETIVOS

OBJETIVO GENERAL

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

OBJETIVOS ESPECÍFICOS

- Establecer un banco de trabajo con requisitos mínimos para el desarrollo de actividades del desarrollo del seminario.
- Replicar escenarios de instrucción entre máquinas que permita afectar la información de la máquina atacada.
- Fortalecer la seguridad de la máquina afectada por el payload.
- Establecer recomendaciones de seguridad sobre el escenario propuesto.

DESARROLLO DE LA ACTIVIDAD

ETAPA 1

PREGUNTA 1

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.

Ley 1273 de 2009

La Ley 1273 de 2009, es la más conocida "Ley de Delitos Informáticos" que tiene aplicabilidad en Colombia, es una legislación que aborda los delitos relacionados con el uso indebido de tecnologías de la información y la comunicación, donde a su vez, tiene el propósito de establecer normas para prevenir, sancionar y combatir los delitos electrónicos y cibernéticos en el país.

- **Artículo 269A: Acceso abusivo a un sistema informático.**

Establece las sanciones para la violación y uso de datos personales sin ningún tipo de autorización y establece diferentes grados de pena dependiendo de la naturaleza del que comete el delito y la relación con su actividad.

- **Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación**

Establece medidas y sanciones para el personal que impide o obstaculiza el acceso a un sistema informático o una red de comunicación, esto incluyendo la información y datos contenidos sin estar autorizado para realizarlo.

- **Artículo 269C: Interceptación de datos informáticos.**

Indica las sanciones que tendrá toda persona que, sin orden judicial previa, intercepte datos informáticos desde su origen, destino o dentro de un sistema informático, o intercepte emisiones electromagnéticas de un sistema informático que los transporte.

- **Artículo 269D: Daño Informático.**

Establece las medidas preventivas de toda persona que destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

- **Artículo 269E: Uso de software malicioso.**

Trata sobre el uso indebido de software dañino. Se refiere a acciones como crear, vender, distribuir o enviar software malicioso o programas de computadora que causen daño, sin tener la autorización para hacerlo.

- **Artículo 269F: Violación de datos personales.**

Se refiere a la violación de datos personales. Esta se produce cuando alguien, sin autorización, obtiene, recopila, roba, ofrece, vende, cambia, envía, compra, intercepta, divulga, altera o utiliza códigos o información personal que está guardada en archivos, bases de datos u otros medios similares, con el propósito de beneficiarse a sí mismo o a otra persona.

- **Artículo 269G: Suplantación de sitios web para capturar datos personales.**

Habla sobre la suplantación de sitios web con el fin de obtener datos personales de manera ilegal. Esto ocurre cuando alguien crea, desarrolla, vende, ejecuta, programa o envía páginas web, enlaces o ventanas emergentes con intenciones ilícitas y sin la autorización adecuada, con el objetivo de engañar y recopilar información personal de forma indebida.

- **Artículo 269H: Circunstancias de agravación punitiva**

Establece los escenarios y circunstancias que agravan las penas previstas en los artículos anteriores y que puede hacer de que el tiempo y/o monto estipulado como multa sea superior.

- **Artículo 269I: Hurto por medios informáticos y semejantes.**

Recuerda sobre el hurto mediante el uso de medios informáticos indicados en artículos anteriormente mencionados, pero en este caso teniendo en cuenta el uso de medios informáticos para la realización de estas actividades.

- **Artículo 269J: Transferencia no consentida de activos.**

Se refiere a la transferencia no autorizada de activos. Esto ocurre cuando alguien, con el objetivo de obtener ganancias, utiliza trucos informáticos o artimañas

similares para lograr que se transfiera un activo sin el consentimiento de otra persona, causándole daño. Esto aplica siempre que el acto no esté considerado como un delito más grave en términos de pena.

Ley 1581 de 2012

La Ley 1581 de 2012 en Colombia, también conocida como la "Ley de Protección de Datos Personales", regula el tratamiento de la información personal en el país. Esta ley establece los principios, deberes y derechos relacionados con la recolección, almacenamiento, uso, circulación y protección de datos personales por parte de entidades públicas y privadas en Colombia.

La Ley 1581 tiene como objetivo principal garantizar la privacidad y el control de las personas sobre sus datos personales, promoviendo la responsabilidad y transparencia en el manejo de la información. Entre sus disposiciones se incluyen requerimientos para obtener el consentimiento informado de las personas antes de recolectar sus datos, medidas de seguridad para proteger la información, y reglas para la circulación y transferencia de datos personales, entre otros aspectos.

Esta ley busca proteger los derechos de los ciudadanos en relación con su información personal y fomentar prácticas responsables por parte de las organizaciones que tratan con esos datos.

Adicionalmente, entre los aspectos más importantes de la Ley 1581 de 2012 se encuentran la definición de datos personales, los derechos que tienen los titulares de los datos, las obligaciones de las entidades que manejan datos personales, las medidas de seguridad que deben ser implementadas, y las sanciones por el incumplimiento de la ley.

Por otra parte, se verifica cuáles son las sanciones y el ente regulador de esta ley, donde se identifican los siguientes artículos que brindan mayor detalle al respecto:

Artículo 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones[1]:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

[1] LEY 1581 de 2012 Congreso de la República de Colombia [Anónimo]. Inicio | Sede Electrónica – Secretaria General [página web]. [Consultado el 8, agosto, 2023]. Disponible en Internet: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>.

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Artículo 24. Criterios para graduar las sanciones. Las sanciones por infracciones a las que se refieren el artículo anterior se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables[2]:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) La reincidencia en la comisión de la infracción;

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;

e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;

f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

[2] LEY 1581 de 2012 Congreso de la República de Colombia [Anónimo]. Inicio | Sede Electrónica - Secretaria General [página web]. [Consultado el 8, agosto, 2023]. Disponible en Internet: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>.

PREGUNTA 2

2. El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

ETAPAS DEL PENTESTING

Las pruebas de penetración, o pruebas de penetración, son el proceso sistemático de simulación de ataques cibernéticos en sistemas, aplicaciones o redes para identificar vulnerabilidades y evaluar la seguridad de esos sistemas. Las fases más comunes identificadas en las pruebas de penetración son:

- **Recopilación de información (reconocimiento):** durante esta fase, se recopila información sobre el objetivo de la prueba de penetración. Esto puede incluir la identificación de sistemas, servicios, direcciones IP, nombres de dominio, información de contacto y otra información relevante que puede usarse para identificar posibles puntos de entrada.

- **Análisis de la información:** una vez que se recopila la información, se analiza para identificar posibles vulnerabilidades y posibles vectores de ataque. Esto puede incluir la identificación de sistemas obsoletos, servicios obsoletos o configuraciones inseguras. Detección de vulnerabilidades: esta fase utiliza herramientas automatizadas y técnicas manuales para buscar vulnerabilidades conocidas dentro del objetivo. Estas vulnerabilidades pueden ser brechas de seguridad de software, configuraciones incorrectas o debilidades de la red.

- **Explotación:** cuando se encuentra una vulnerabilidad explotable, se intenta comprometer un sistema o aplicación utilizando técnicas de explotación. El objetivo es demostrar que la vulnerabilidad se puede explotar para obtener acceso no autorizado.

- **Escalada de privilegios:** una vez dentro del sistema, el pentester puede intentar elevar los privilegios para obtener un acceso más profundo y amplio al objetivo. Para hacer esto, debe otorgarle privilegios más altos de lo normal.

- **Movimiento lateral:** si el objetivo de esta fase es una red, el probador de penetración se moverá lateralmente a través de la red en busca de otros sistemas o segmentos que puedan estar comprometidos. Esto simula las acciones que podría realizar un atacante real después de obtener acceso al sistema.

- **Mantenimiento del acceso:** una vez que se obtiene el acceso, un probador de penetración puede intentar mantener ese acceso para demostrar que un atacante puede permanecer persistentemente en el sistema. Esto puede implicar la creación de puertas traseras o la manipulación de cuentas de usuario.

- **Documentación y presentación:** al final de la prueba de penetración, se documentan todas las etapas del proceso, incluidas las vulnerabilidades descubiertas, las técnicas utilizadas y los resultados obtenidos. A continuación, se presenta a los clientes un informe detallado que describe las vulnerabilidades identificadas y proporciona recomendaciones para mejorar la seguridad.

- **Limpieza y recuperación:** después de completar una prueba de penetración, se debe realizar una limpieza completa de cualquier acceso o modificación al sistema de destino. Esto es fundamental para garantizar que la prueba no deje rastro y el sistema vuelva a su estado original.

Etapa "Footprinting"

Esta etapa también es llamada como "reconocimiento" o "recopilación de inteligencia") y es el primer paso en el proceso de prueba de penetración, recopilando información sobre objetivos que se evalúan desde una perspectiva de seguridad. El objetivo principal de esta fase es obtener una descripción general de los sistemas, la infraestructura y los activos de la organización que están sujetos a las pruebas de penetración, que pueden estar orientadas hacia la realización de algunas de las siguientes actividades.

- **Recopilación de información pública**: Se reúne información disponible públicamente sobre la organización, como nombres de dominio, direcciones IP, contactos de la empresa, información de registro de dominios y otra información que esté accesible en línea.

- **Búsqueda de información:** Se utilizan motores de búsqueda avanzados y técnicas de búsqueda para recopilar datos adicionales sobre el objetivo, como subdominios, registros de DNS, información de WHOIS, etc.

- **Identificación de rangos de IP:** Se determinan los rangos de direcciones IP que pertenecen a la organización. Esto puede ayudar a identificar posibles puntos de entrada.

- **Exploración de redes sociales:** Se analizan perfiles de redes sociales, sitios web de empleados y otros recursos en línea para recopilar información sobre empleados, tecnologías utilizadas y posibles interacciones de la organización.

- **Descubrimiento de servicios y tecnologías:** Se utilizan herramientas y técnicas para identificar los servicios y las tecnologías que la organización utiliza en su infraestructura, como identificación de puertos abiertos, servicios expuestos y versiones de software.

- **Identificación de vulnerabilidades conocidas**: Se pueden buscar públicamente vulnerabilidades conocidas en los servicios y aplicaciones identificados. Esto ayuda a identificar puntos potenciales de entrada.

- **Búsqueda de información de correo electrónico:** Se buscan direcciones de correo electrónico y patrones de nomenclatura que puedan ser utilizados para realizar ataques de ingeniería social u otros tipos de ataques.

- **Identificación de socios y proveedores:** Se recopila información sobre socios comerciales, proveedores y terceros relacionados con la organización, ya que también podrían representar posibles puntos de entrada.

PREGUNTA 3

¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

Se debe considerar como la etapa más importante ya que de este modo se busca proporcionar una base sólida para las siguientes fases del pentesting, ya que permite a los pentesters comprender mejor la superficie de ataque, los posibles vectores de ataque y los activos críticos que deben ser evaluados. Sin embargo, es importante llevar a cabo esta etapa de manera ética y cumpliendo todas las regulaciones y leyes pertinentes para que las demás etapas del pentesting sean realizadas de forma correcta.

PREGUNTA 4

Aplicaciones utilizadas

Dentro de cada una de las etapas se usan diferentes herramientas y aplicaciones, dentro de las principales se relacionan:

3. Arpag
4. AutoSploit
5. BeEF
6. BugBounty Recon
7. BurpSuite
8. Canvas
9. Dnsmap

10. Dnsrecon
11. Dradis
12. Empire
13. Enumdb
14. Faraday
15. GhostPack
16. Lolbas and Llolbas
17. Metasploit
18. Mimikatz
19. Nessus
20. Netcat
21. Nmap
22. OpenVAS
23. OWASP Zap Proxy
24. PHPSploit
25. Poet
26. PowerHub
27. PowerSploit
28. Pwnat
29. Recon-ng
30. RemoteRecon
31. Routersploit
32. ShellPop
33. Simple Vulnerability Manager
34. SPARTA
35. SQLMap
36. SubFinder
37. Swap_Digger
38. TheFatRat
39. Vega
40. Xarp

PREGUNTA 5

Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

METASPLOIT

La función principal del metasploit es permitir a los profesionales de seguridad evaluar la vulnerabilidad de sistemas informáticos, aplicaciones y redes, y tomar medidas para mejorar su seguridad.

Metasploit ofrece una plataforma integral para descubrir, explotar y validar vulnerabilidades en entornos controlados y autorizados. Aquí hay un resumen de cómo funciona Metasploit
Dentro de su funcionamiento se puede establecer:

- **Recolección de información:** En la etapa inicial, los usuarios pueden utilizar Metasploit para recopilar información sobre objetivos potenciales, como sistemas, servicios y aplicaciones. Esta información se utiliza para identificar posibles vulnerabilidades y puntos de entrada.

- **Selección de módulos:** Metasploit cuenta con una amplia colección de módulos predefinidos, que incluyen exploits, payloads, post-explotation modules y más. Los módulos son piezas de código que realizan tareas específicas, como explotar vulnerabilidades, obtener acceso a sistemas, ejecutar comandos, etc.

- **Configuración del exploit:** Los usuarios seleccionan un exploit específico que corresponda a la vulnerabilidad que desean explotar. Luego, ajustan la configuración del exploit, como la dirección IP del objetivo y los puertos involucrados.

- **Selección de payload:** Un payload es el código que se ejecutará en el sistema objetivo una vez que se explote la vulnerabilidad. Los payloads pueden ser desde simples shells hasta herramientas más avanzadas de control remoto. Los usuarios eligen un payload que se adapte a sus objetivos y necesidades.

- **Explotación:** Una vez que se ha configurado el exploit y el payload, Metasploit intenta explotar la vulnerabilidad en el objetivo. Si la vulnerabilidad es explotable, el payload se envía al sistema objetivo, lo que permite al atacante obtener acceso o control sobre el sistema.

- **Control y post-explotación:** Después de una exitosa explotación, el atacante puede tener control sobre el sistema objetivo. Metasploit ofrece una variedad de módulos post-explotación que permiten realizar tareas adicionales, como enumeración de usuarios, recopilación de información, pivote de red y más.

- **Limpieza y eliminación:** En un contexto ético, es importante que los profesionales de seguridad eliminen cualquier acceso no autorizado y restaurar el sistema objetivo a su estado original. Esto se hace utilizando módulos de limpieza y eliminación proporcionados por Metasploit.

- **Reporte y documentación:** Al finalizar la prueba de penetración, se deben documentar todas las etapas, resultados y hallazgos. Esto ayuda a los equipos de seguridad y a la organización a comprender las vulnerabilidades y tomar medidas para mitigar los riesgos.

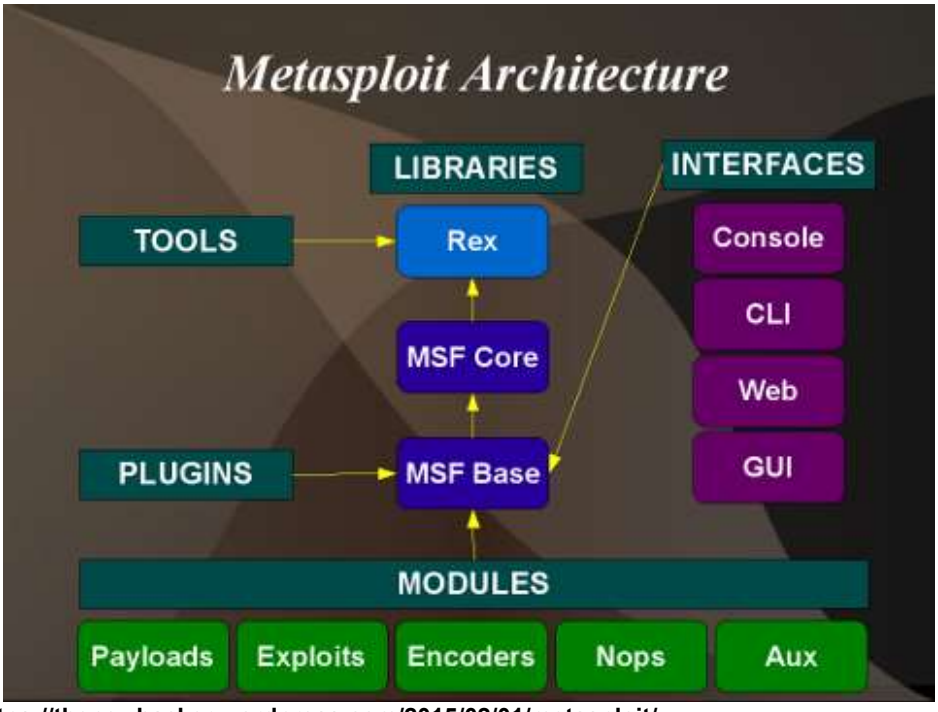
Arquitectura Metasploit

La arquitectura de Metasploit está determinada de la siguiente manera[3]:

- **Módulo Payloads:** Nos proporciona gran cantidad de códigos "maliciosos" que podremos ejecutar una vez haya tenido éxito el exploit.
- **Módulo Exploits:** Aquí es donde se encuentran todos los exploits disponibles en el framework para conseguir acceso en los sistemas.
- **Módulo Encoders:** Proporciona algorítmos para codificar y ofuscar los payloads que utilizaremos tras haber tenido éxito el exploit.
- **Módulo Nops:** Nos permite realizar u obtener operaciones nop.
- **Módulo Auxiliary:** Permite la interacción de herramientas externas como pueden ser escaners de vulnerabilidades, sniffers, etc… con el framework de Metasploit.

De este modo, se muestra a continuación de forma gráfica de como se ve la arquitectura.

Figura 1 Arquitectura Metasploit



Fuente: https://thenewhacker.wordpress.com/2015/02/01/metasploit/

[3] METASPLOIT FRAMEWORK [Anónimo]. SystemExposed [página web]. [Consultado el 10, agosto, 2023]. Disponible en Internet: <https://systemexposed.blogspot.com/2014/01/metasploit-framework.html>.

PREGUNTA 6

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.

Dentro del proceso descrito en este apartado usted como experto en ciberseguridad debe buscar y documentar lo siguiente:

¿QUÉ ES UN CVE Y SU ESTRUCTURA?

Es un sistema público y estandarizado para identificar y catalogar de manera clara y uniforme las brechas de seguridad en los sistemas informáticos y software.

El propósito del sistema CVE es proporcionar una forma coherente de hacer referencia a vulnerabilidades específicas y facilitar la comunicación, el seguimiento y la gestión de vulnerabilidades por parte de la comunidad de ciberseguridad.

Donde la estructura esta definida como año, número de secuencia e identificador único, que de forma más detallada relacionan:

1. **Año:** El número de año en el que se emitió el CVE. Por ejemplo, "2023" en el caso de una vulnerabilidad identificada en 2023.

2. **Número secuencial:** Un número asignado secuencialmente a las vulnerabilidades dentro de un año determinado. Este número se inicia desde "1" al comienzo de cada año y se incrementa a medida que se identifican nuevas vulnerabilidades.

3. **Identificador único:** Este es el sufijo alfanumérico único que completa el CVE. Puede contener letras y números, y a menudo se selecciona para que sea relevante para la vulnerabilidad en cuestión.

Adicionalmente, se asocia con una descripción detallada de la vulnerabilidad, incluidos detalles como el software afectado, la versión específica, una descripción del problema, la posible gravedad y cualquier otra información relevante.

https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

La página relacionada es un banco de información respecto a diferentes exploit, donde indica la información del tipo, plataforma y autor, que esta relacionada con las listas relacionadas en la CVE.

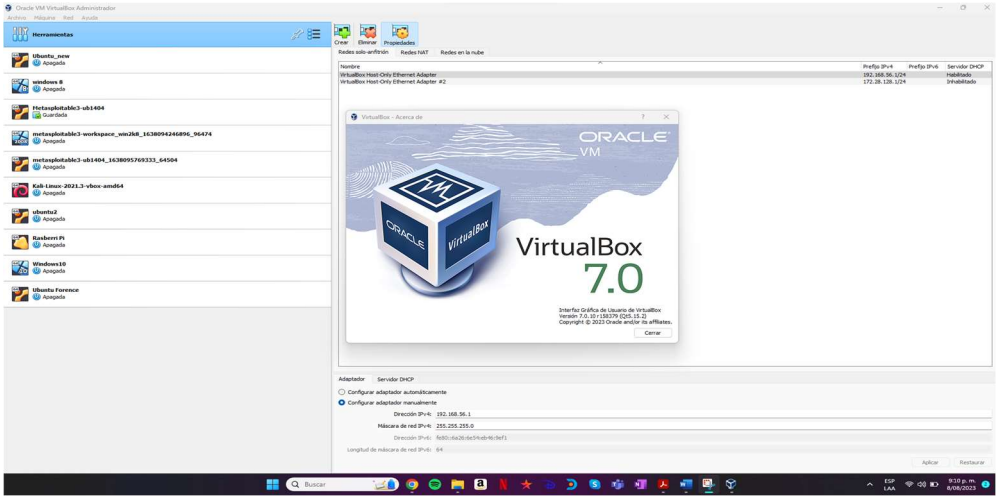
Además de ser una aplicación web que reúne bases de datos públicas con exploits para vulnerabilidades conocidas, en lo que contribuyen los usuarios. Dichos exploits

pueden ser consultados, descargados y utilizados por pentesters de todo el mundo de forma gratuita para mejorar la calidad de sus auditorías de ciberseguridad.

BANCO DE TRABAJO

Para el desarrollo del banco de trabajo se cuenta con la última versión de la máquina virtual Virtualbox 7.0

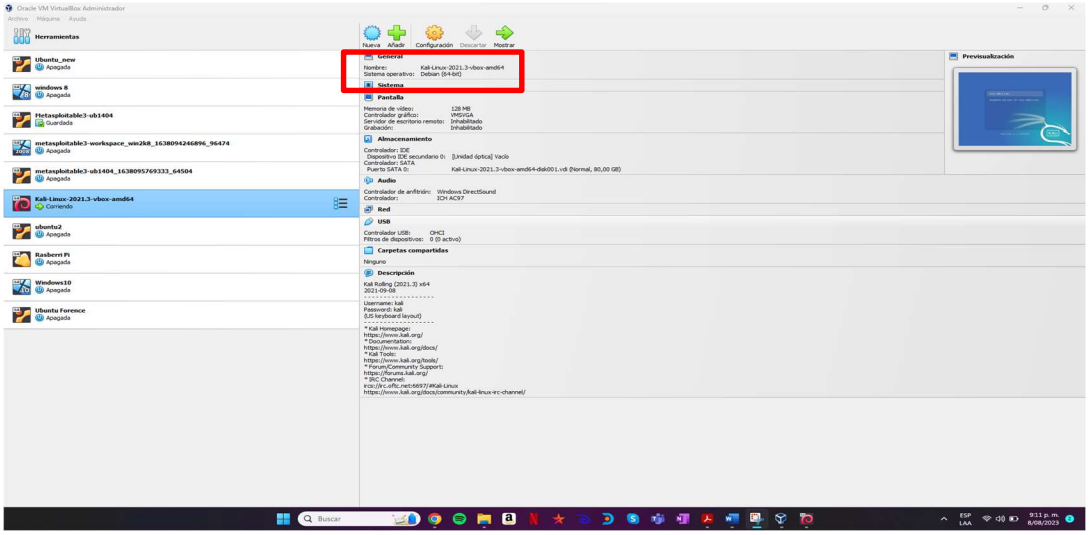
Figura 2 Versión Máquina Virtual



Fuente: John Rativa

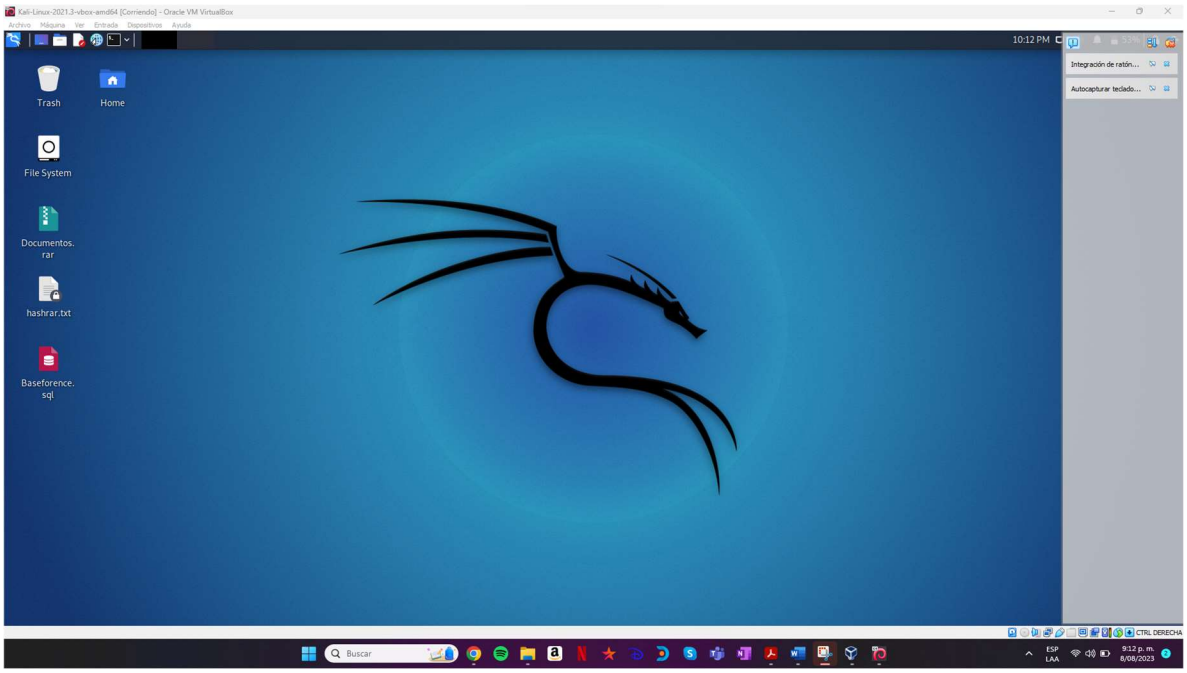
Donde, para el desarrollo del banco de trabajo se cuenta con una máquina Kali Linux totalmente funcional

Figura 3 Kali Linux 1



Fuente: John Rativa

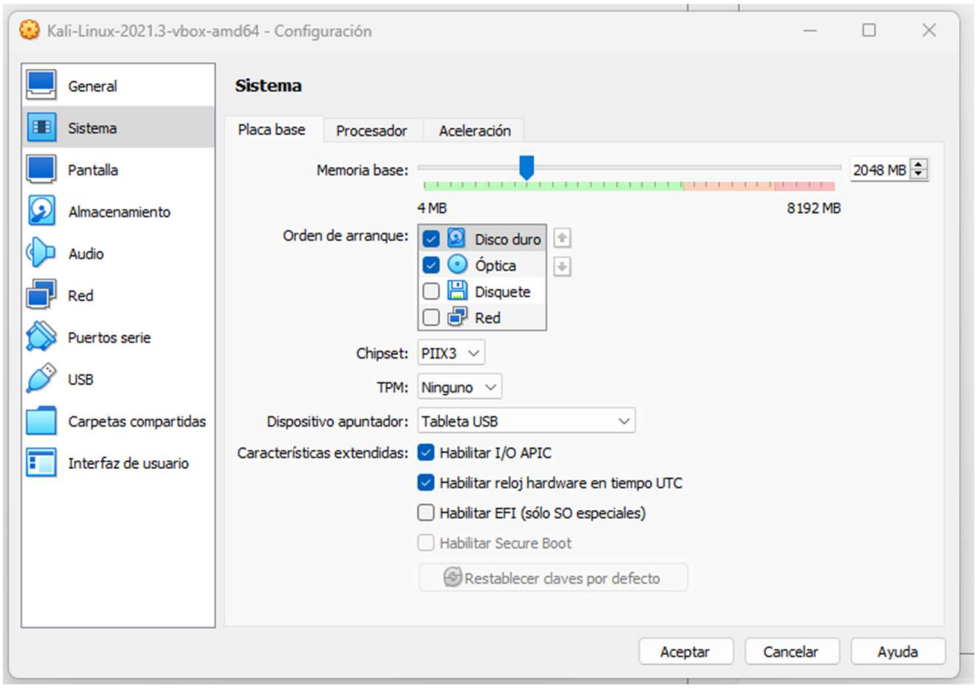
Figura 4 Kali Linux 2



Fuente: John Rativa

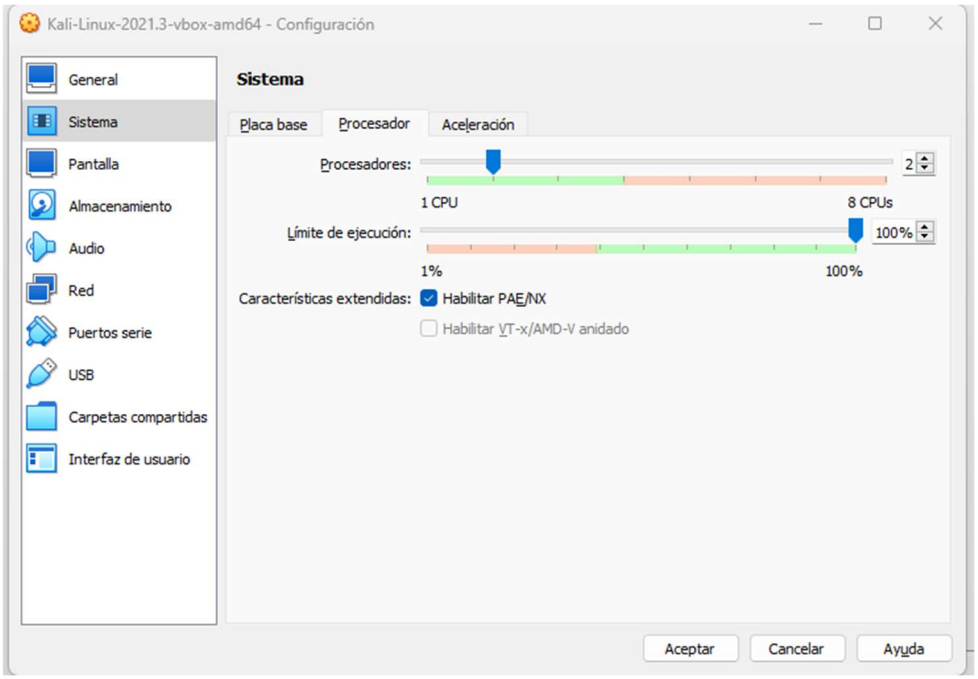
Relacionando los parámetros de configuración:

Figura 5 Kali Linux Confi_1



Fuente: John Rativa

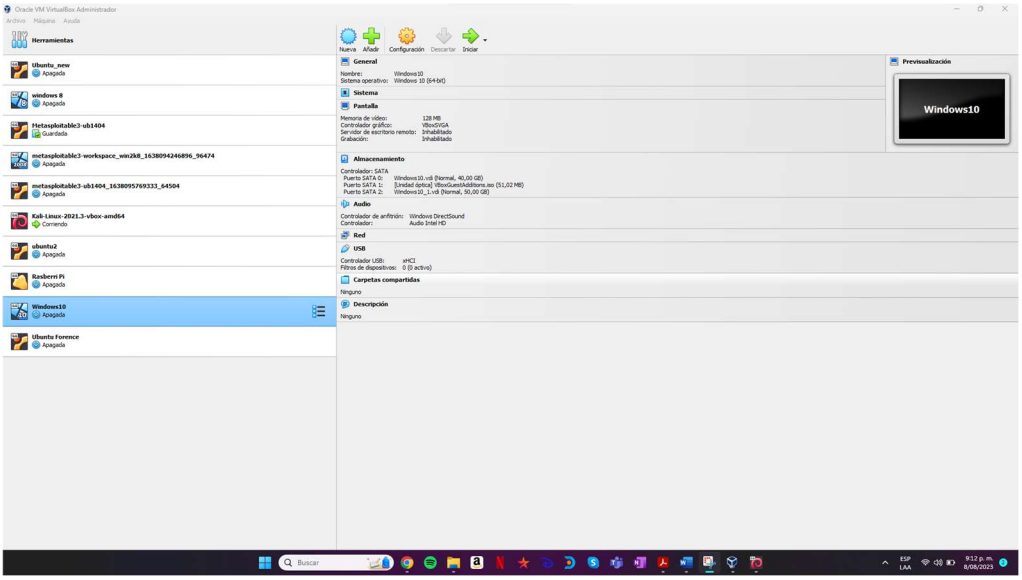
Figura 6 Kali Linux Confi_2



Fuente: John Rativa

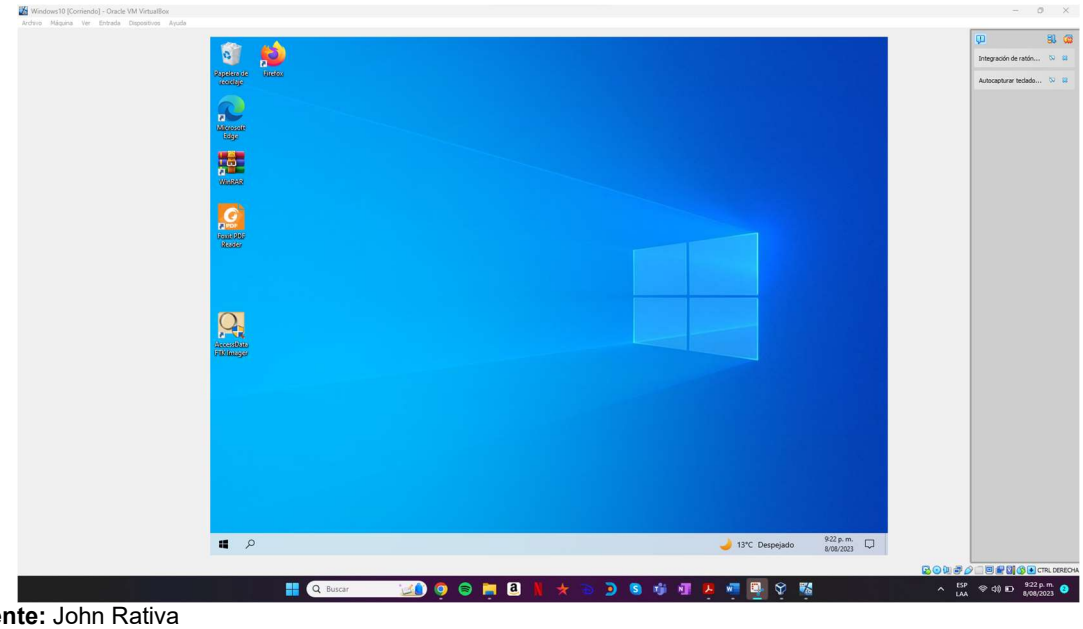
Así mismo, se cuenta con una máquina Windows 10 totalmente funcional.

Figura 7 Windows 10_1



Fuente: John Rativa

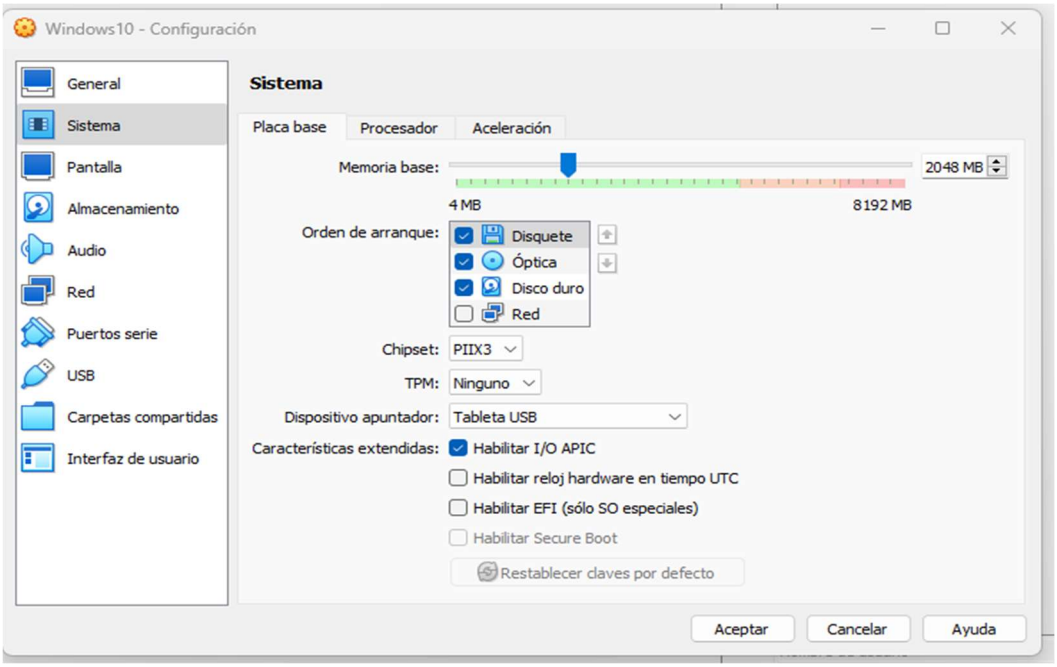
Figura 8 Windows 10_2



Fuente: John Rativa

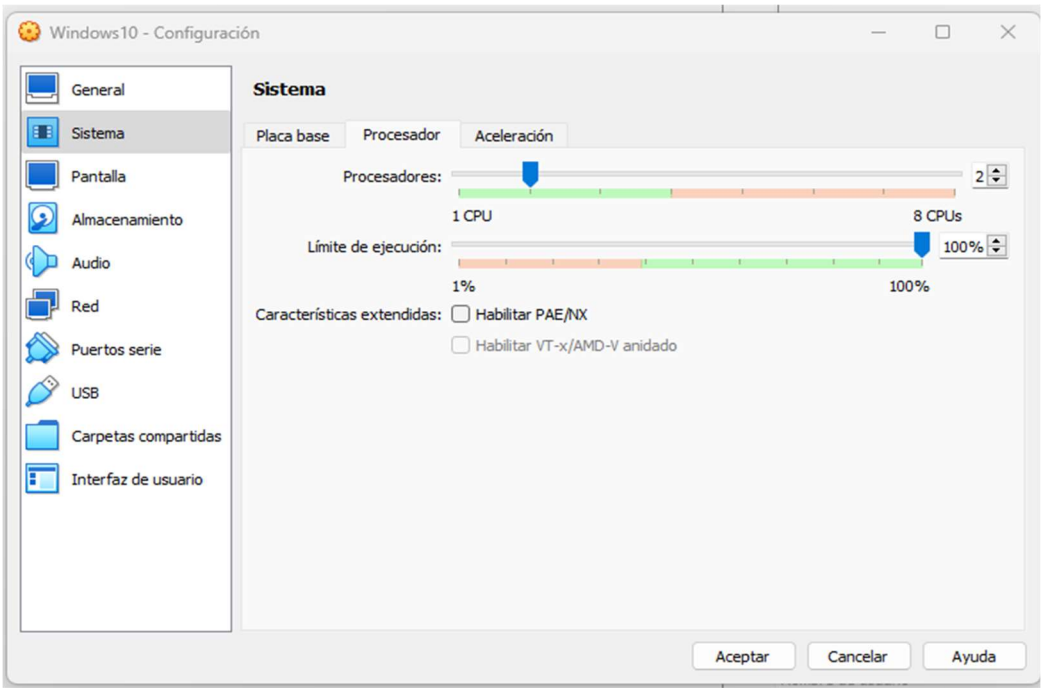
Se relaciona la información de la configuración de la máquina win10

Figura 9 Windows Confi_1



Fuente: John Rativa

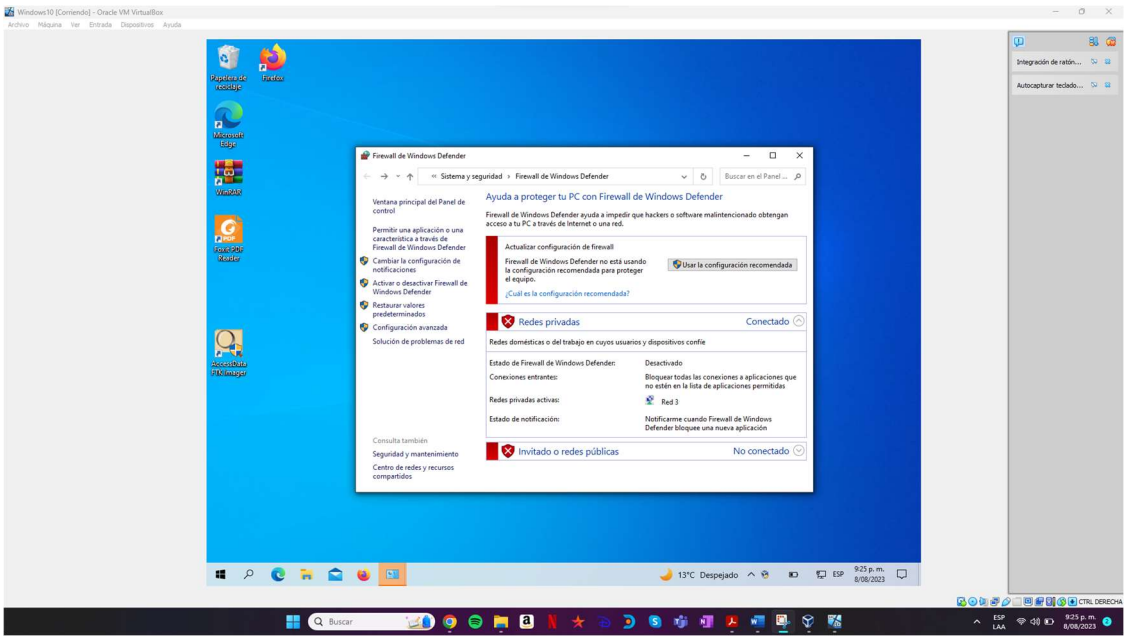
Figura 10 Windows Confi_2



Fuente: John Rativa

Donde, se realiza la desactivación de todo protocolo de seguridad, en este caso del firewall

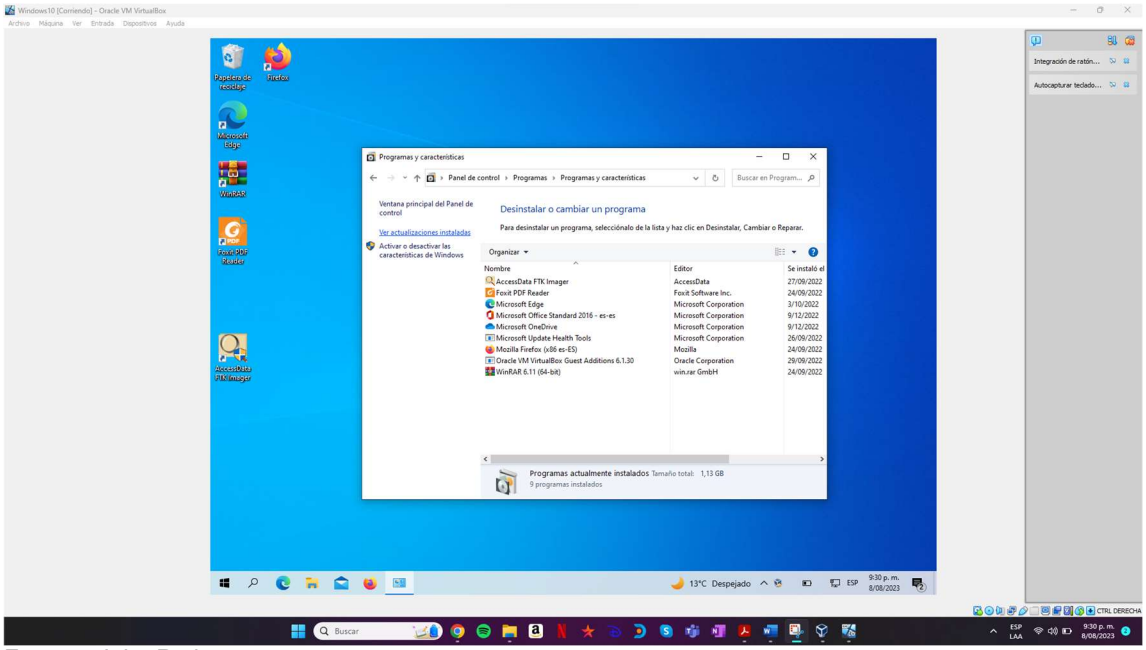
Figura 11 Firewall Off_Win10



Fuente: John Rativa

Como también se confirma que no se cuenta con herramientas de antivirus.

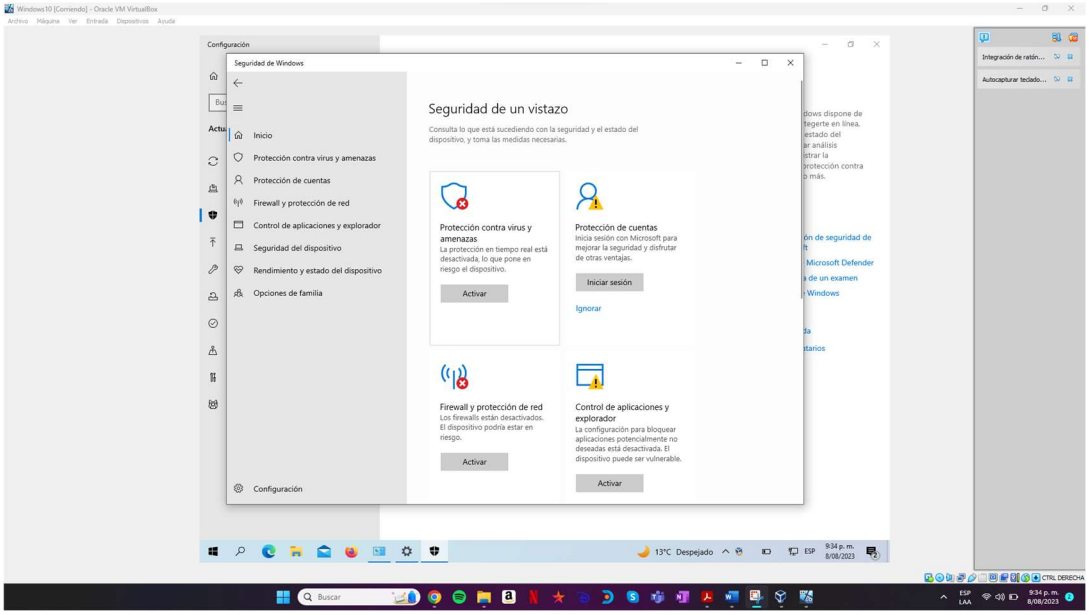
Figura 12 Antivirus Off_Win10



Fuente: John Rativa

Y la desactivación de toda la seguridad de Windows Defender

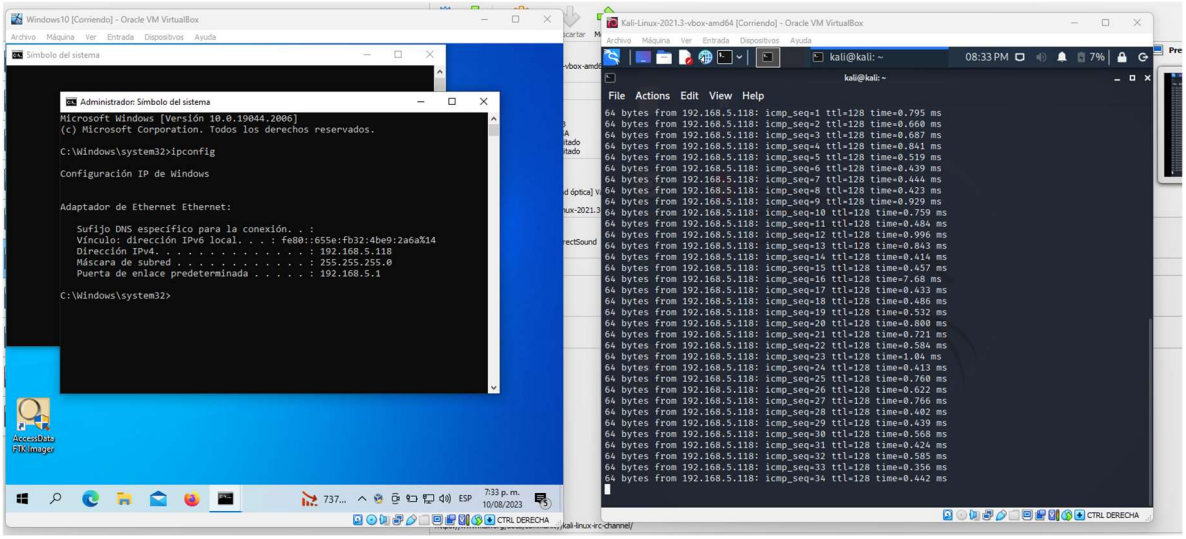
Figura 13 WinDefender Off_Win10



Fuente: John Rativa

Por último, se realiza verificación de comunicación entre las máquinas virtuales, realizando ping entre ellas y logrando envió correcto de paquetes. Confirmando de este modo que existe conexión exitosa.

Figura 14 Conexión OK Máquinas



Fuente: John Rativa

ETAPA 2

PREGUNTA 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.

R:/
Dentro del proceso de análisis de los dos anexos definidos para ser consultados, he identificado los siguientes párrafos o textos dentro del anexo, que desde mi punto de vista considero que no se tornan del todo legales.

a. Clausula primera: la **información confidencial:** Donde parte de su texto indica “la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.”

En mi opinión, prohibir la denuncia o divulgación de procesos ilegales plantea importantes dilemas éticos y legales. Por un lado, el derecho a la libertad de

expresión ya la información transparente es fundamental en una sociedad democrática. Poder denunciar actividades ilegales es fundamental para prevenir el abuso, la corrupción y las violaciones de los derechos humanos.

Por otro lado, hay situaciones en las que la confidencialidad de cierta información es necesaria para proteger las investigaciones en curso, la seguridad nacional o la privacidad personal. Sin embargo, en este tipo de escenarios es importante tener la potestad para poder divulgar o informar sobre cualquier proceso ilegal y que pueda constituir un proceso mal realizado, donde a su vez puede generar un delito mayor o que incurra en multas o sanciones.

De este modo, es importante que existan mecanismos apropiados para denunciar de manera confidencial las malas conductas y proteger a quienes se atrevan a denunciar conductas ilegales o inmorales.

b. Cuarta. **Obligaciones de la parte receptora:** “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”.

Hay que tener en cuenta que la prohibición de denunciar actividades sospechosas que impliquen obtener información sobre otros plantea problemas importantes de privacidad y seguridad de los datos.

Donde, si se minimiza esa la capacidad de denunciar actividades sospechosas, que son fundamentales para prevenir y combatir los delitos cibernéticos, el fraude y los abusos relacionados con la adquisición ilegal de información personal, se puede generar mayores brechas o mayor cantidad de delitos por cometer que estamos permitiendo por no realizar un debido actuar.

Así mismo, también es importante contar con mecanismos para informar posibles violaciones de la privacidad y la seguridad de los datos, especialmente cuando se trata de actividades ilegales.

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

Dentro de mi punto de vista, considero, en este punto, que si bien es un aspecto importante de la responsabilidad y la cooperación con las fuerzas del orden en situaciones legales en caso de una investigación o proceso donde se vea afectada la información. Esta responsabilidad no debería estar asociada solo a la persona que acepta las cláusulas si no a la compañía, ya que para muchos ítems son los “dueños” de la información, pero en caso de alguna novedad retiran toda responsabilidad.

De este modo, responder ante las autoridades competentes en un proceso de allanamiento implica asumir la responsabilidad por la información en su poder y cooperar plenamente con las investigaciones en curso. Esto puede contribuir a la aplicación efectiva de la justicia y al esclarecimiento de situaciones que involucren actividades ilegales o sospechosas que debería ser tomada desde todas las partes y no solo desde una parte de las personas involucradas.

PREGUNTA 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.

R:/
Dentro del análisis del anexo 3, logro identificar los siguientes escenarios, que considero pueden tener algún proceso ilegal o que puede afectar la forma en que son evaluados.

a. **Clausula Segunda.** Definición de información confidencial, indica **"**datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos".

En este caso la ley que puede estar presente es la Ley 1273 de 2009, puntualmente en su artículo 269ª, que está relacionado con:

- **Artículo 269A: Acceso abusivo a un sistema informático.**

Establece las sanciones para la violación y uso de datos personales sin ningún tipo de autorización y establece diferentes grados de pena dependiendo de la naturaleza del que comete el delito y la relación con su actividad.

De este modo, se esta abusando del acceso a los sistemas informáticos al captar, interceptar de forma no autorizada y abusiva información de datos secretos y que son considerados dentro del anexo como "datos de cruzadas". Incumpliendo el uso correcto de la información e incurriendo en penas económicas y legales.

b. **Clausula Cuarta.** Obligaciones de la parte receptora: "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."

Para este escenario también está relacionada directamente la Ley 1273 de 2009, en su artículo 269C, que indica:

- **Artículo 269C: Interceptación de datos informáticos.**

Indica las sanciones que tendrá toda persona que, sin orden judicial previa, intercepte datos informáticos desde su origen, destino o dentro de un sistema informático, o intercepte emisiones electromagnéticas de un sistema informático que los transporte.

Donde, según lo que se indica en las clausulas del anexo, se tiene conocimiento de la intervención inapropiada de la información de terceros y que de acuerdo con lo indicado no se debe notificar sobre estos hechos inadecuados antes las autorizades, generando incumplimiento en el correcto tratamiento de la información y ampliando la posibilidad de que se puedan presentar estos escenarios donde se realiza interceptación de los datos sin ningún control.

PREGUNTA 3

El sueldo para los puestos de Red team y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

R:/
Como profesional integral que me considero, mi respuesta es No aceptaría la propuesta realizada, así el salario fuera lo bastante llamativo como lo es en este escenario hipotético. Donde, tendría para llegar a esta respuesta he tenido en cuenta varios aspectos, como lo son:

Por mi parte no estaría dispuesto a participar en actividades ilegales o éticamente cuestionables y más teniendo en previo conocimiento de que estos escenarios que pueden presentar considerando algunos de los deberes que se asumen a partir de la adquisición de la tarjeta profesional como “Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder”[4], que en este sentido no se tendría dicha libertad para denunciar estos delitos, incumpliendo este ítem.

[4] CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. (20, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

Así mismo, se estaría apoyando y dando mayor facilidad para que la empresa siga generando procesos ilegales, donde se debe tener en cuenta que entre las prohibiciones generales que uno adquiere se encuentran:

- Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley.[5]

Por otra parte, si entramos a verificar más detalladamente los deberes especiales que se aceptan al ser profesional y aún más al contar con tarjeta profesional para ejercer respectivamente, se incumpliría directamente con el ítem “Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”. De este modo, aceptando la realización de tareas fuera de un escenario adecuado y que por contrato estaría dispuesto a realizar.

Por último, hay que tener en cuenta, que el incumplimiento de uno o varios ítems relacionados anteriormente, pueden dar como resultado la generación de faltas leves hasta graves, que pueden ser las causantes de la generación de diferentes escenarios comprobables como:

a. Amonestación Escrita, en el caso de las faltas leves.
b. Suspensión de la Matrícula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios.
c. La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

De este modo, por mi parte, considero importante siempre tener en cuenta los pros y contras de aceptar algún tipo de condición en los contratos a firmar y de este modo dar cumplimiento de la mejor manera al desarrollo de las actividades y dar cumplimiento al código de ética para el desarrollo de las funciones adquiridas al iniciar a ser profesional de ingeniería.

PREGUNTA 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.

[5] CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. (20, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

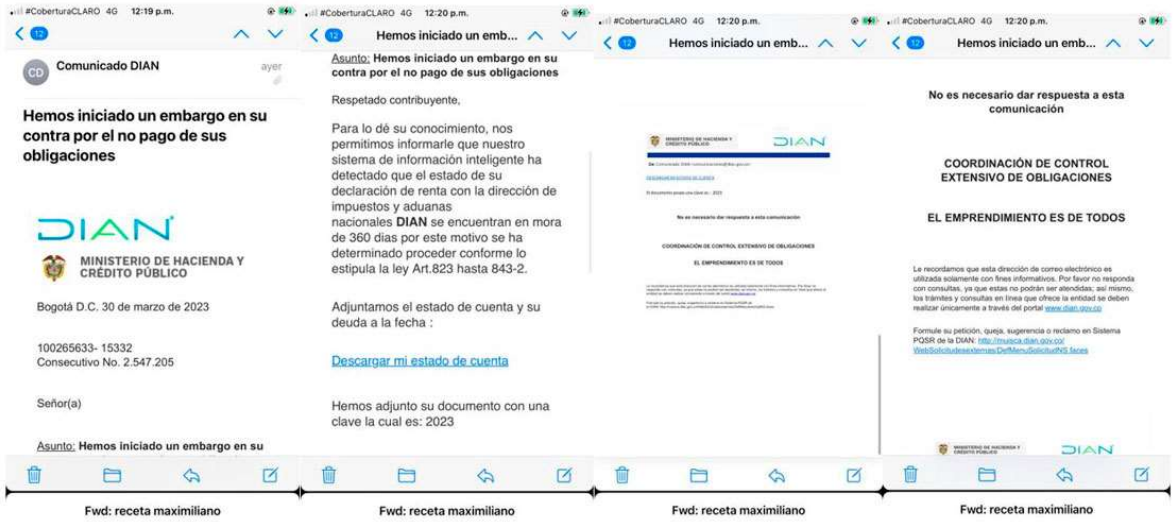
R:/

Título de la noticia “No se deje engañar, mediante correos y llamadas fraudulentas a nombre de directivos de la DIAN pretenden estafar a los ciudadanos.”

La noticia es tomada de la página oficial de la DIAN, https://www.dian.gov.co/Prensa/Paginas/NG-Comunicado-de-Prensa-024-2023.aspx

En este caso la noticia esta alertando sobre el uso inadecuado de correos electrónicos, llamadas y mensajes a nombre de la DIAN, solicitando ingresar a link fraudulentos, ingresar información, descargar archivos entre otros, como se muestra de ejemplo:

Figura 15 DIAN Noticia



Fuente: John Rativa

El modo de operación que se describe es: “inescrupulosos hacen llamadas a los ciudadanos suplantando la identidad de directivos, ofreciendo el supuesto servicio de devolución automática de saldos a favor en impuestos nacionales. En estas llamadas solicitan información personal de los ciudadanos para obtener datos de cuentas bancarias, con el fin de acceder a estas y cometer delitos como robo o estafa.”[6]

Dentro del escenario propuesto y evidenciado, se tiene en cuenta que se está incumpliendo la Ley 1273 de 2009, en los artículos 269G y 269I, que están relacionados con:

[6] PRENSA Comunicado de Prensa No. 024 [Anónimo]. Dirección de Impuestos y Aduanas Nacionales - DIAN [página web]. (20, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.dian.gov.co/Prensa/Paginas/NG-Comunicado-de-Prensa-024-2023.aspx>.

- **Artículo 269G: Suplantación de sitios web para capturar datos personales.**

Habla sobre la suplantación de sitios web con el fin de obtener datos personales de manera ilegal. Esto ocurre cuando alguien crea, desarrolla, vende, ejecuta, programa o envía páginas web, enlaces o ventanas emergentes con intenciones ilícitas y sin la autorización adecuada, con el objetivo de engañar y recopilar información personal de forma indebida.

- **Artículo 269I: Hurto por medios informáticos y semejantes.**

Recuerda sobre el hurto mediante el uso de medios informáticos indicados en artículos anteriormente mencionados, pero en este caso teniendo en cuenta el uso de medios informáticos para la realización de estas actividades.

Ahora bien, desde mi punto de vista se puede considerar que la suplantación de identidad de sitios web y la incitación al robo son tácticas ciberdelincuentes que plantean graves problemas de seguridad y privacidad, que, si se ven desde una perspectiva ética y legal, estas acciones se consideran ilegales y dañinas para las personas y organizaciones involucradas.

Así mismo, la suplantación de identidad de sitios web implica la creación de páginas web falsas que parecen sitios web legítimos para engañar a los usuarios para que obtengan credenciales o información personal es algo que cada vez se ha vuelto más común, desde la creación de un mensaje de texto, correo electrónico o incluso actualmente con el uso de WhatsApp. Donde el principal objetivo es conducir al robo de datos confidenciales, como contraseñas, información financiera e información personal.

También, en estos escenarios de robo de información, los atacantes generalmente se hacen pasar por organizaciones confiables, como bancos o corporaciones, para engañar a las víctimas para que accedan a datos de forma más fácil y con apariencia de “seguridad”.

Desde una perspectiva ética y social, estos actos son reprobables porque abusan de la confianza de las personas y pueden causar daños económicos y emocionales. Además, estas actividades dañan la seguridad en línea y la confianza en las transacciones digitales.

Por último, legalmente estos actos se consideran delitos informáticos y están sujetos a sanciones legales que hemos ido observando con las leyes de protección de datos personales.

ETAPA 3

PREGUNTA 1

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

R:/

Para el desarrollo de la actividad planteada en el anexo 4, inicialmente, se cuenta con la herramienta Virtualbox, donde se cuenta con dos máquinas preinstaladas, la primera una máquina con Windows10, donde tenemos deshabilitados todos los servicios que tienen que ver con la seguridad del dispositivo, es decir, el firewall, antivirus como aplicación y Windows defender de la máquina, desde cada aspecto que permite salvaguardar la herramienta.

Por otra parte, la segunda máquina cuenta con una configuración básica de un Kali Linux con las ultimas actualizaciones disponibles y la herramienta metasploit disponible para realizar cada paso a paso del desarrollo de la actividad.

Una vez, se cuenta con cada respectiva máquina, se realiza la creación de un .exe por la herramienta Msfvenom, donde se establece la configuración de los parámetros de conexión que van a ser utilizados en el ataque, es decir, la IP de la máquina que va a ser la atacante, el puerto de conexión habilitado para la conexión y el tipo de sistema operativo que va a ser vulnerado en la ejecución de la actividad.

Se utiliza adicionalmente, la herramienta WhatsApp web para realizar el transporte del .exe generado con la herramienta Msfvenom entre cada una de las máquinas virtuales del ejercicio.

Por otra parte, se hace uso de un exploit que sirva de intermediario de escucha entre las máquinas, para usar del mismo modo un meterpreter para la realización de diferentes líneas de comandos para realizar cambios o obtención de información entre la máquina atacante y la máquina atacada.

También, se realiza uso de las herramientas de creación de texto como block de notas y Word para la realización del documento que va a ser afectado en la ejecución del escenario propuesto.

PREGUNTA 2

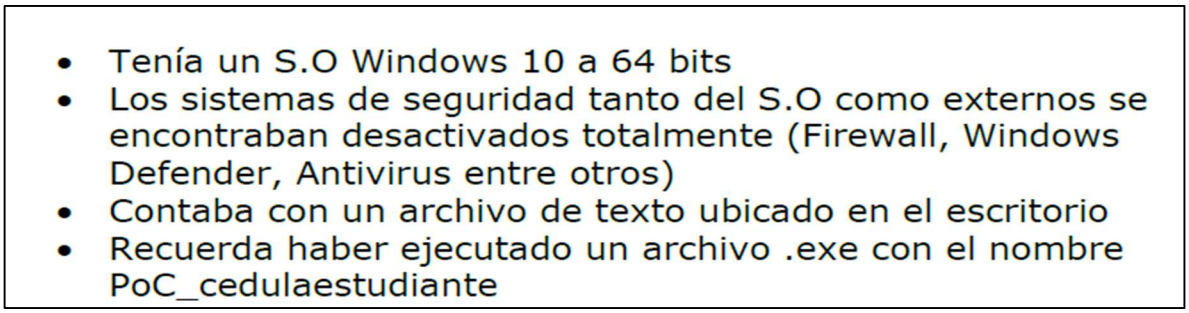
A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 10 X64.

R:/
Dentro del anexo donde se describe el escenario propuesto, inicialmente se indica “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.” De este modo, se establece que en la máquina fue borrada información del escritorio, el cual es el archivo particular que se nombra y que pudo tener fallas en la seguridad de esta.

Como segundo atributo, también se nombra que “dato
bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.” De este modo, se establece que el método de infección de la máquina que dio acceso a una máquina atacante fue la ejecución del archivo (PoCseminario.exe) que fue descargado y ejecutado por un funcionario desde el uso de la herramienta de WhatsApp.

Como tercer atributo, se cuenta con la información general de la máquina relacionada a continuación:

Figura 16 información Sistema WIN10



Fuente: John Rativa

Donde, acorde con lo anterior, aparte de contar con la información de la ejecución del fichero “.exe”, se establece que se encontraba desactivo todo lo relacionado con la seguridad del equipo que fue atacado.

PREGUNTA 3

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”? ¿Qué puerto abre la aplicación específica en el anexo?

R:/
Para la identificación de fallos de seguridad en la máquina de Windows 10 se puede evaluar desde dos puntos de vista, el primero, la identificación de vulnerabilidades

y seguridad que nos muestra Windows cuando se cuenta con todos sistemas de protección abajo, donde se genera alertas de que la máquina no se encuentra segura y puede sufrir alguna afectación y en algunas ocasiones se vuelve a habilitar automáticamente la revisión en tiempo real que identifica este tipo de archivos sospechosos y los elimina antes de poder ser ejecutadas o los bloquea para ejecución.

El segundo punto de vista es desde la máquina atacante al usar el metasploit que se logró comunicar entre las máquinas con la creación del playload, que de este modo permite escuchar la máquina atacada y conocer sobre otras vulnerabilidades disponibles y la información del sistema.

Por último, para el desarrollo de la actividad, el puerto por el cual se realiza la conexión exitosa entre las máquinas y que es el puerto abierto para la conexión es el 443, que dentro del ejercicio es nombrado como LPORT.

PREGUNTA 4

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

R:/
Dentro del análisis del escenario presentado, se evidencia que la máquina Windows inicialmente tuvo una afectación en perdida de información, ya que se expone que solo hubo eliminación de un archivo en el escenario presentado. Sin embargo, los ataques de robo de datos o eliminación de archivos en Windows 10 pueden afectar gravemente la seguridad e integridad de sus datos y sistemas.

Por tal motivo, relaciono algunas de las afectaciones en las que puede verse directamente involucrado en un ataque.

- **Pérdida de datos:** si un atacante elimina con éxito archivos importantes o roba información confidencial, es posible que pierda datos importantes como documentos, imágenes, videos, contraseñas y otros archivos importantes.

- **Compromiso de privacidad:** la pérdida de información personal o confidencial puede comprometer su privacidad y seguridad y generar que los atacantes pueden utilizar estos datos para cometer robo de identidad, extorsión o suplantación de identidad.

- **Fallo del sistema:** acciones de eliminación de archivos importantes del sistema o cambiar configuraciones importantes puede provocar que el sistema operativo falle. Esto puede provocar fallos, pantallazos azules u otros problemas que afecten negativamente a la productividad.

- **Pérdidas financieras:** Dependiendo del tipo de ataque, puede sufrir pérdidas financieras importantes. Por ejemplo, si le roban la información de su tarjeta de crédito o es víctima de un ataque de ransomware, puede sufrir pérdidas financieras directas.

- **Riesgo de distribución de malware:** muchos ataques de robo de datos o eliminación de archivos implican el uso de malware para llevar a cabo sus operaciones. Esto puede permitir que el malware se propague a su sistema, dañando aún más el rendimiento y la seguridad de su sistema.

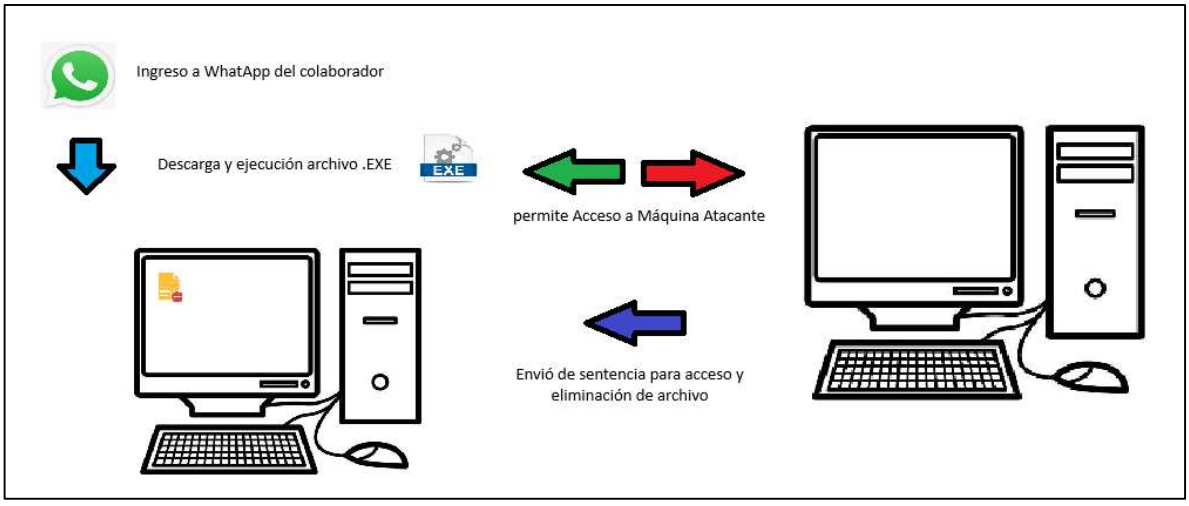
- **Compromiso de seguridad:** un ataque exitoso puede indicar que la seguridad del sistema operativo se ha visto comprometida. Es importante identificar y corregir estas vulnerabilidades para evitar futuros ataques.

- **Daño a la reputación:** si se descubre que sus sistemas han sido víctimas de un ataque, puede dañar la reputación de su empresa o su imagen personal, especialmente si se ven comprometidos datos confidenciales de terceros.

Por este motivo, es importante tener en cuenta que para proteger el sistema operativo Windows 10 de tales ataques, se debe tomar las medidas de seguridad adecuadas, como instalar y mantener software antivirus, actualizar su sistema y sus aplicaciones, realizar copias de seguridad periódicas de los datos importantes y estar al tanto de posibles ataques.

Así mismo, a continuación, se relaciona gráficamente como fue realizado el proceso que le dio acceso a la máquina y que permitió la eliminación de archivos de forma remota.

Figura 17 Acceso Máquina



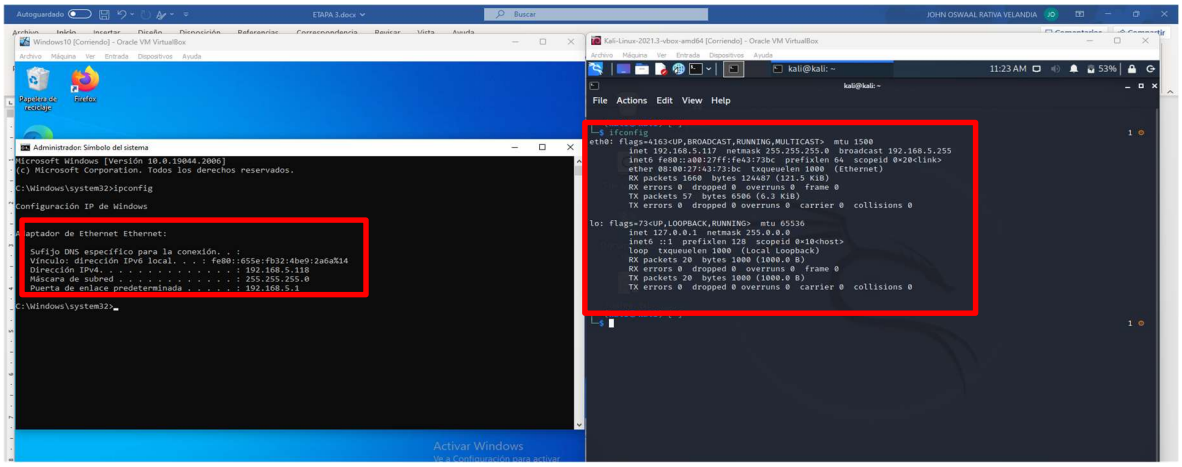
Fuente: John Rativa

PREGUNTA 5

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

Para el desarrollo de la guía inicialmente se cuenta con dos máquinas, donde verificamos sus IPS.

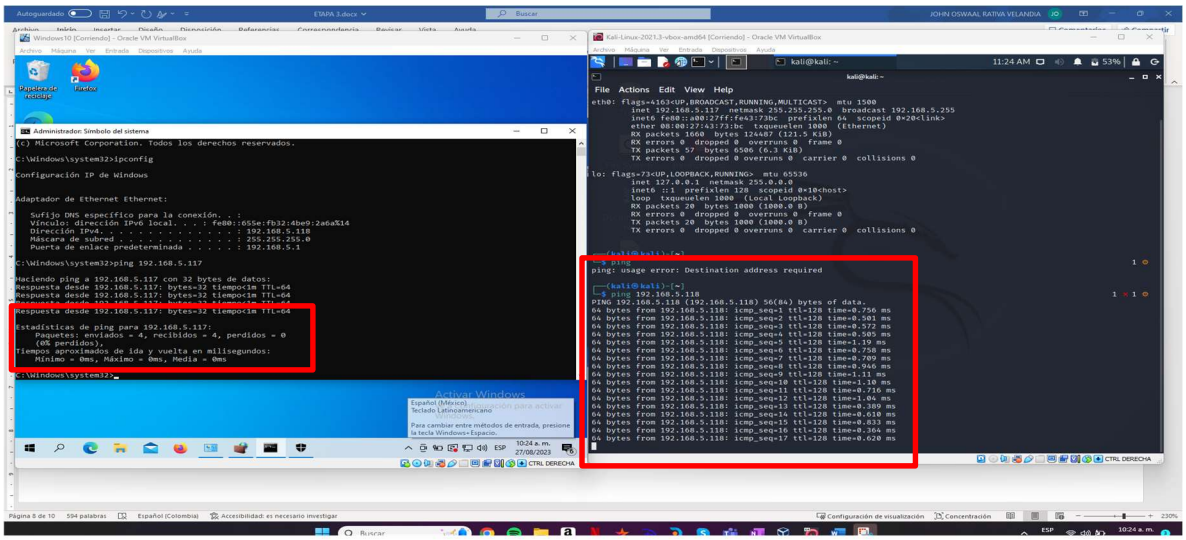
Figura 18 IPS máquinas



Fuente: John Rativa

Una vez se conoce la IP se realiza ping entre las máquinas para confirmar conexión exitosa.

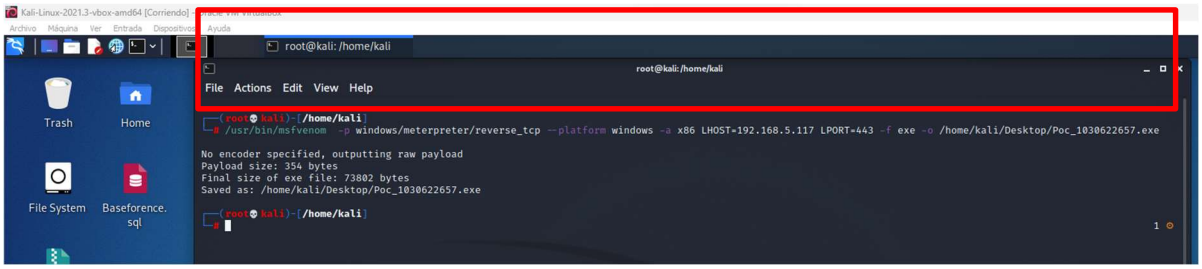
Figura 19 Conexión IP



Fuente: John Rativa

Ahora, se crea el archivo .exe que va permitir la conexión entre máquinas, usando la herramienta MSFVNOM e indicando los parámetros de sistema Operativo, puerto de conexión y nombre del archivo.

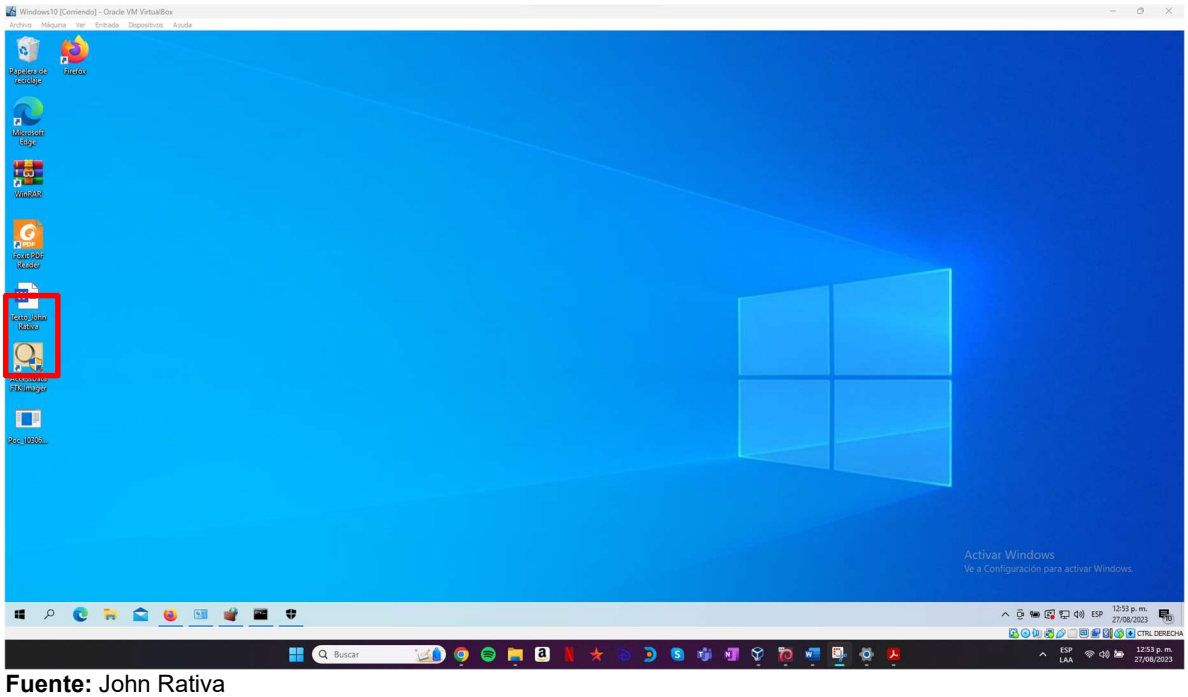
Figura 20 Creación .exe



Fuente: John Rativa

Posteriormente, se realiza paso del archivo a la máquina a ser vulnerada.

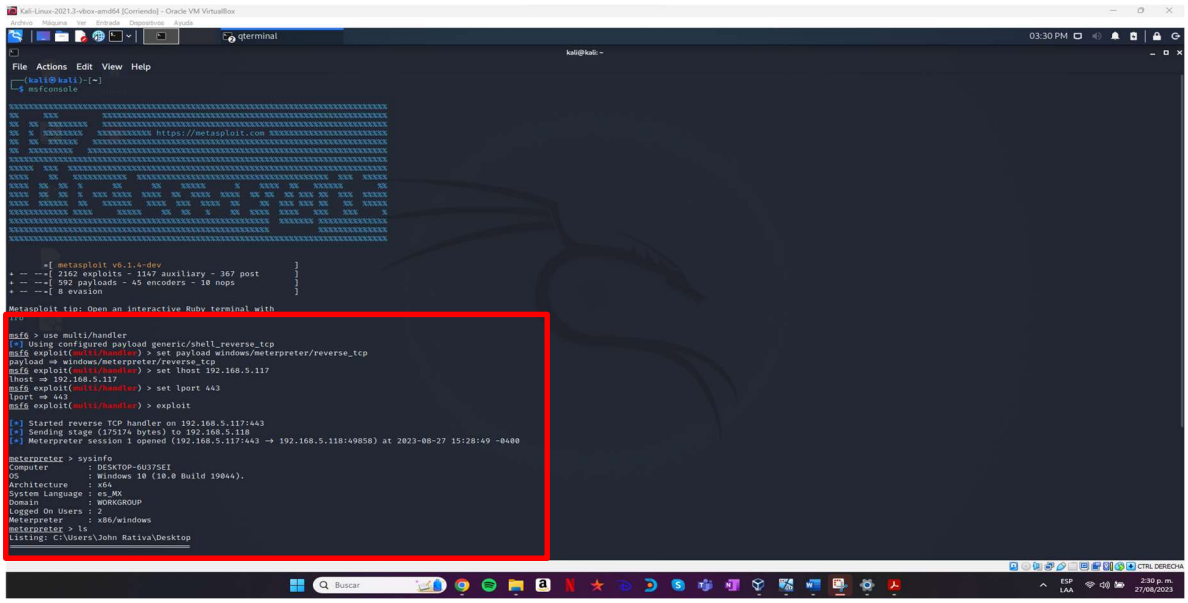
Figura 21 Archivo .exe



Fuente: John Rativa

Una vez se cuenta con el archivo .exe se procede a ejecutar los comandos necesarios para dar apertura a un canal de comunicación entre las máquinas por un metasploit.

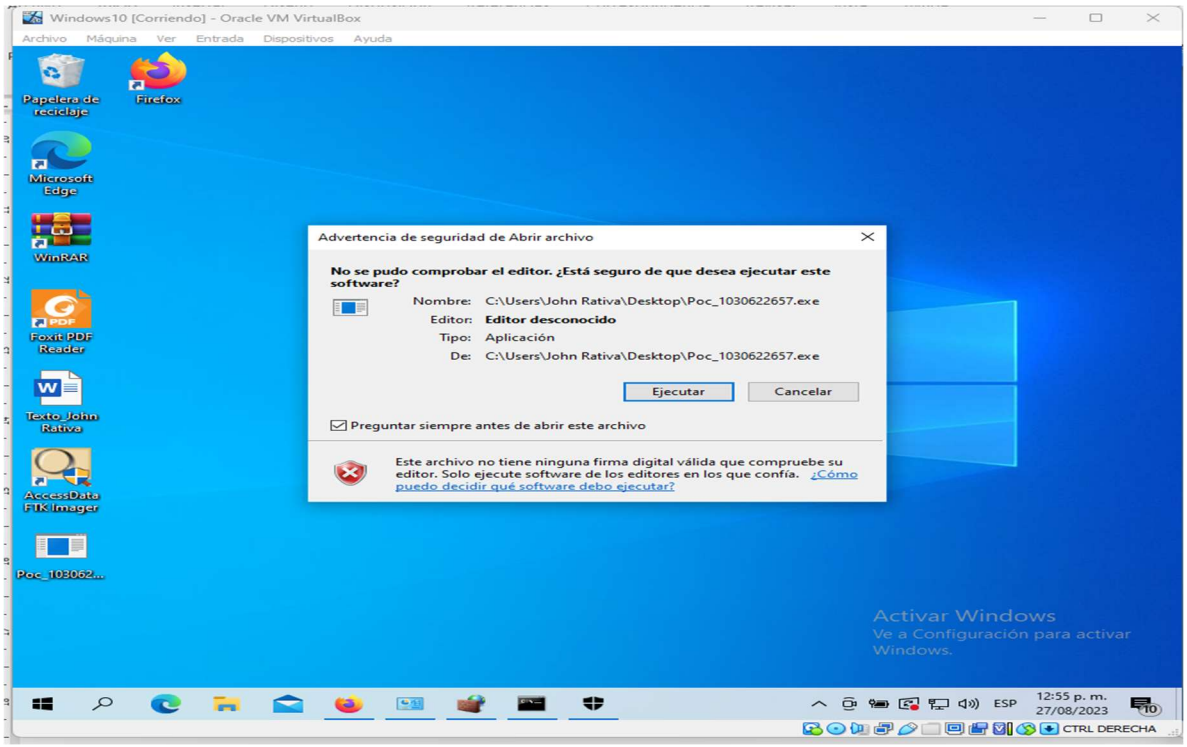
Figura 22 Metasploit



Fuente: John Rativa

Que de una vez se inicia la comunicación, es necesario ejecutar el .exe en la máquina afectada para que se complete la comunicación.

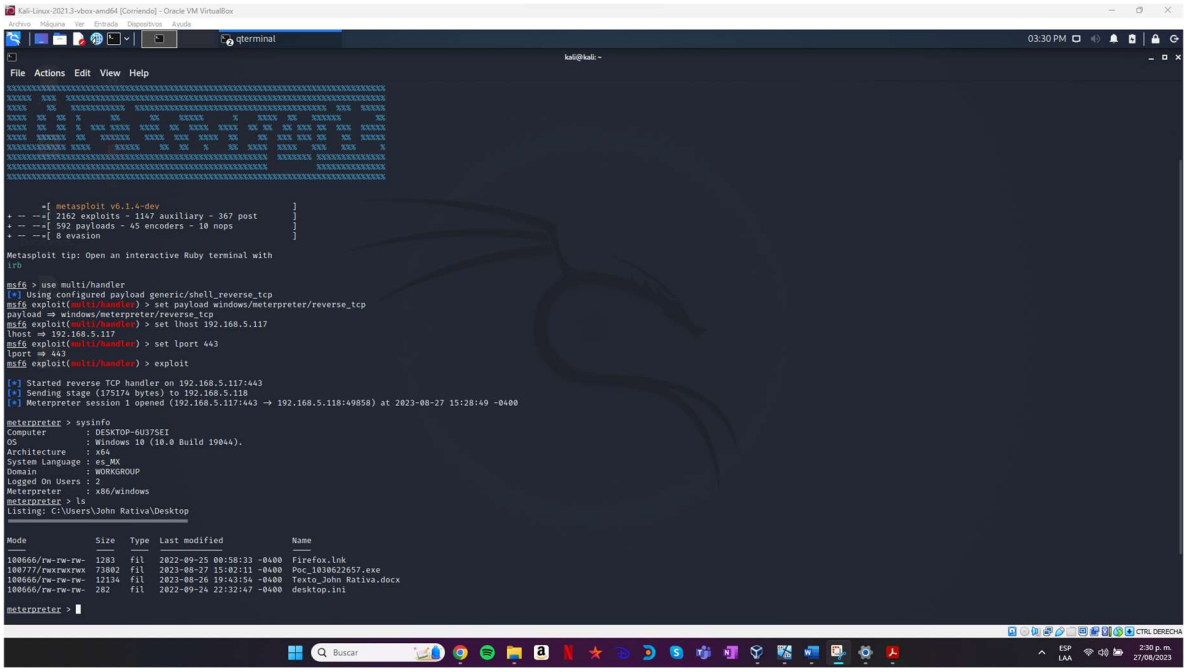
Figura 23 Ejecución archivo Windows



Fuente: John Rativa

Una vez se establece una comunicación exitosa, se realiza uso de la conexión para realizar diferentes actividades en la máquina a atacar, iniciando por listar los documentos que tiene disponibles.

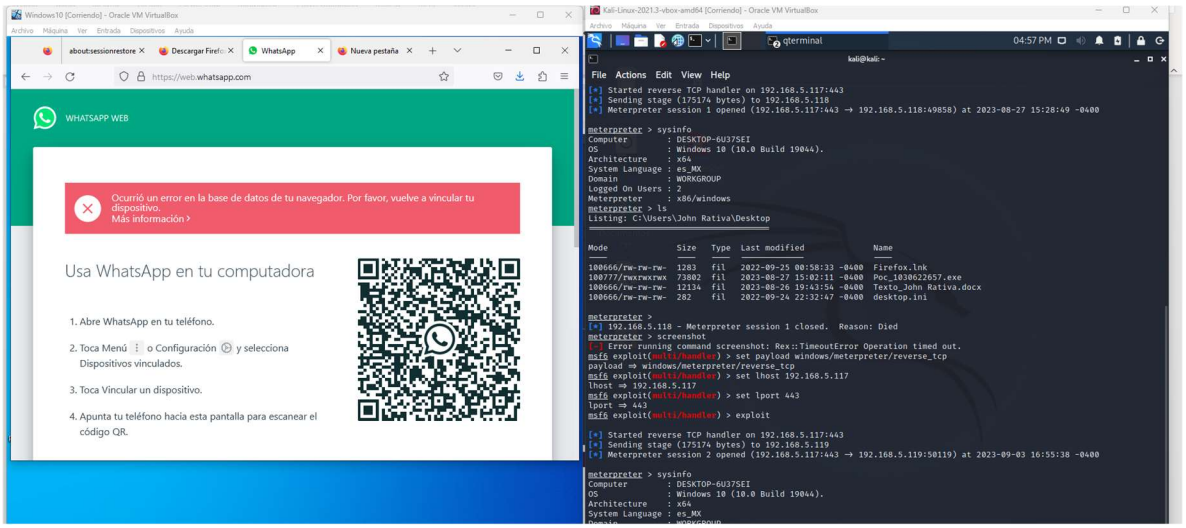
Figura 24 Documentos disponibles



Fuente: John Rativa

Se realiza la prueba de robo de información, realizando una captura de la máquina atacante desde la misma conexión generada.

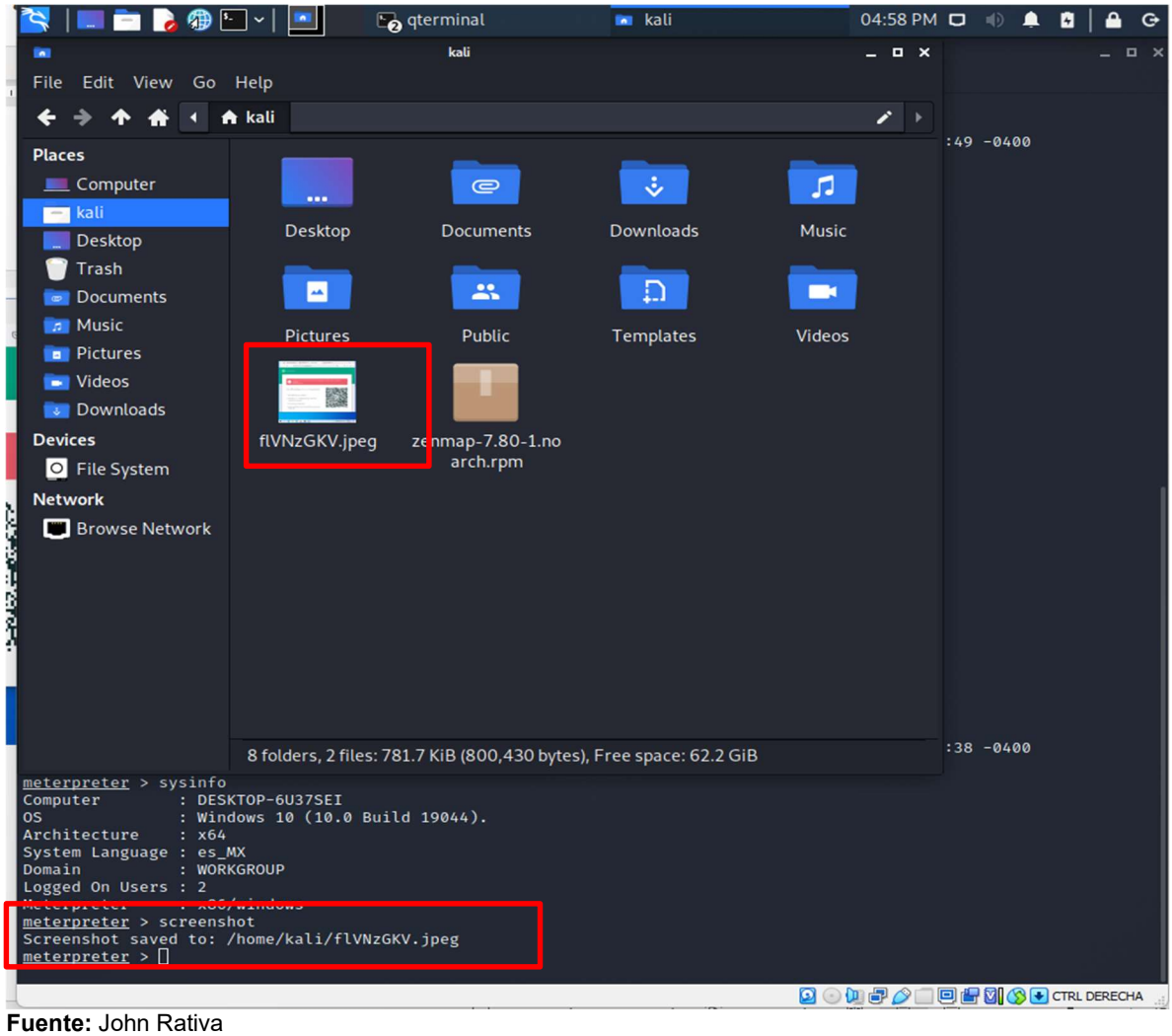
Figura 25 Estado Pantalla antes de Captura



Fuente: John Rativa

Teniendo en cuenta la pantalla donde se encontraba la máquina afectada se verifica y fue guardada exitosamente la pantalla capturada por el meterpreter con el comando “Screanshot”

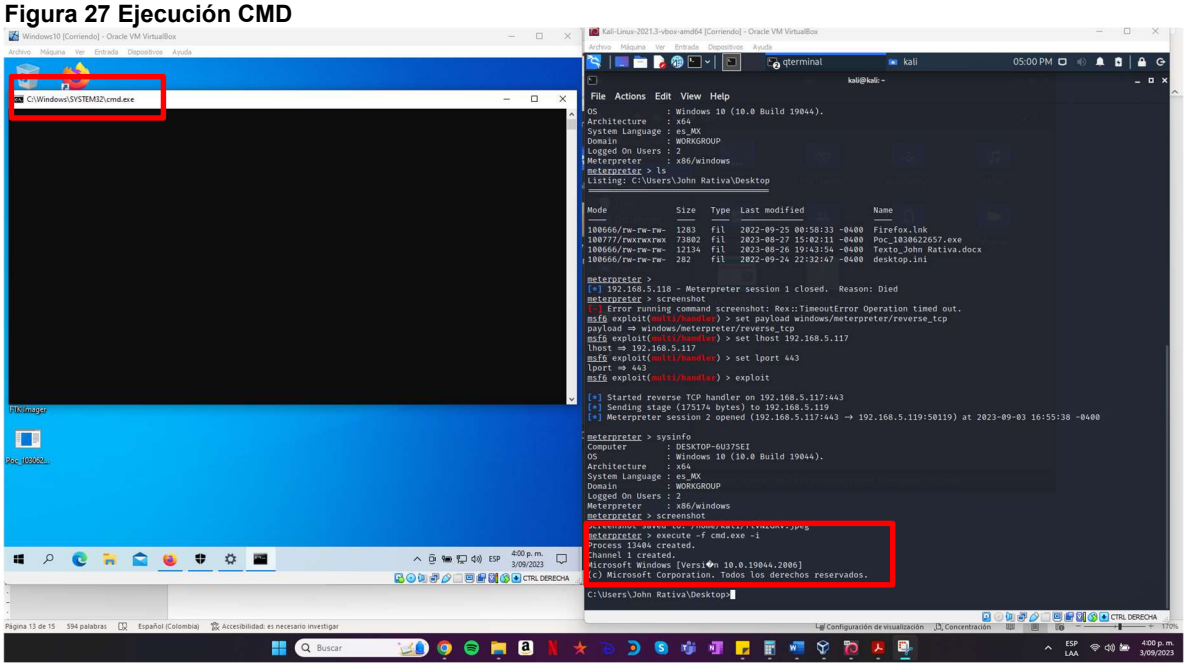
Figura 26 Captura escritorio



Fuente: John Rativa

Se validan otras opciones, donde identificamos la ejecución de consolas de administración de forma remota, con el comando “execute -f cmd.exe -i)

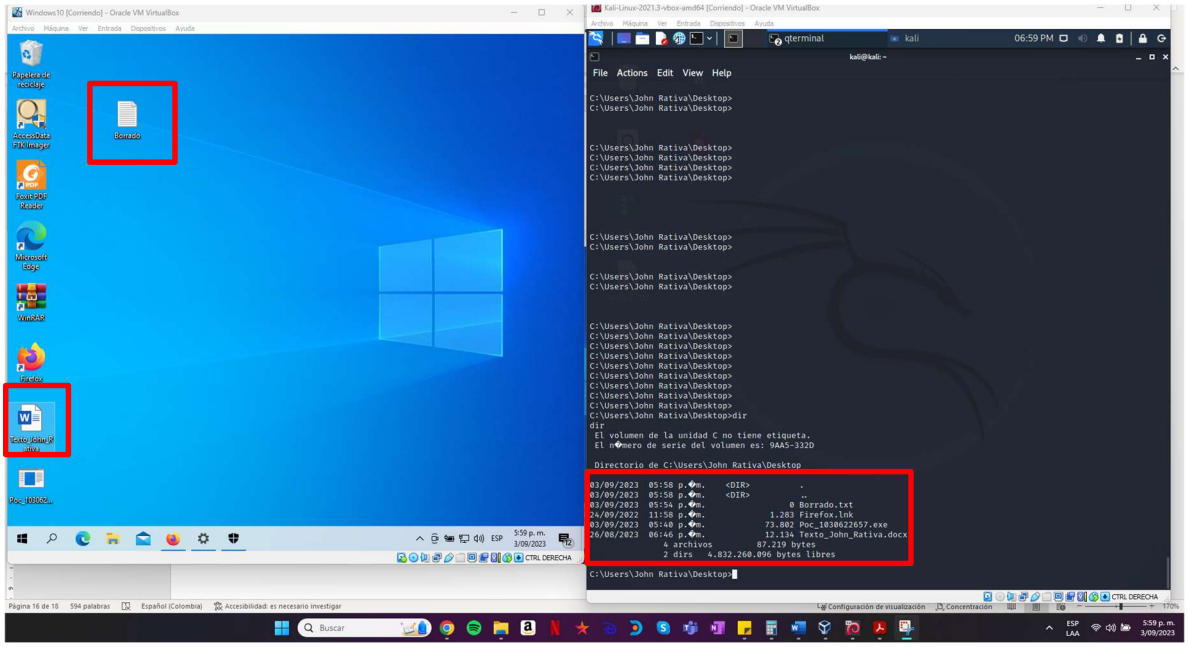
Figura 27 Ejecución CMD



Fuente: John Rativa

Finalmente, se desea verificar las pruebas de borrado realizadas por el atacante en la máquina, por lo cual se creó un segundo archivo .txt para realizar un borrado doble. En este caso, inicialmente se confirma la existencia y ubicación de los archivos.

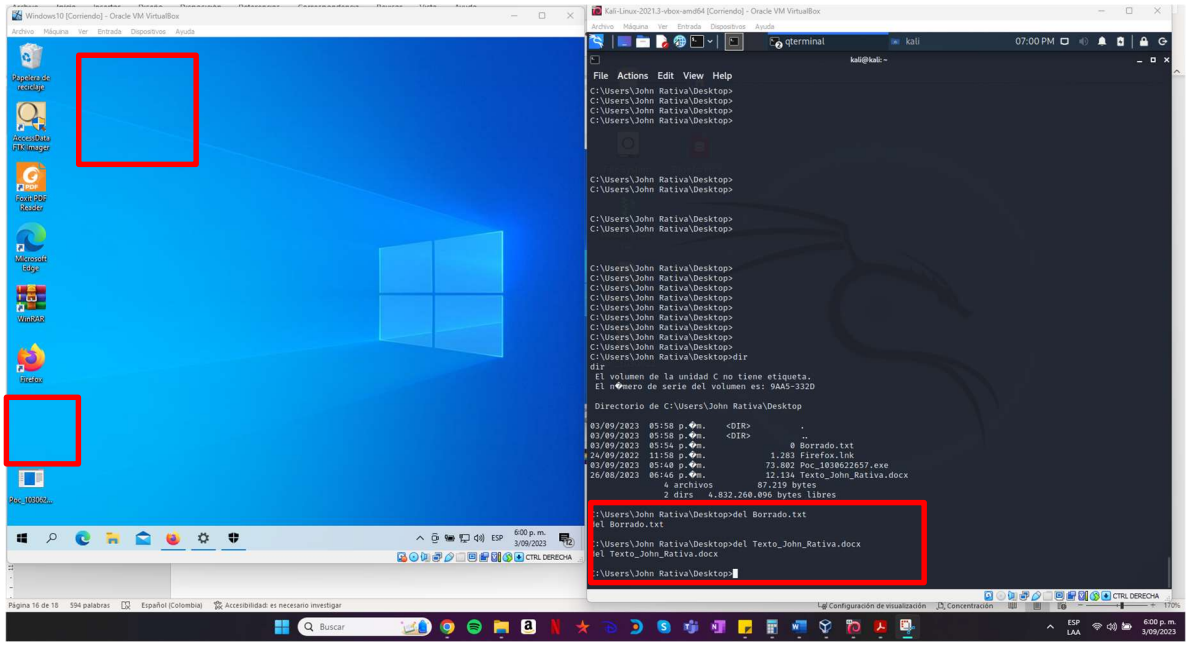
Figura 28 Desktop máquina atacada



Fuente: John Rativa

Donde por medio del comando “del (Nombre del archivo” logramos ejecutar el borrado de los documentos.

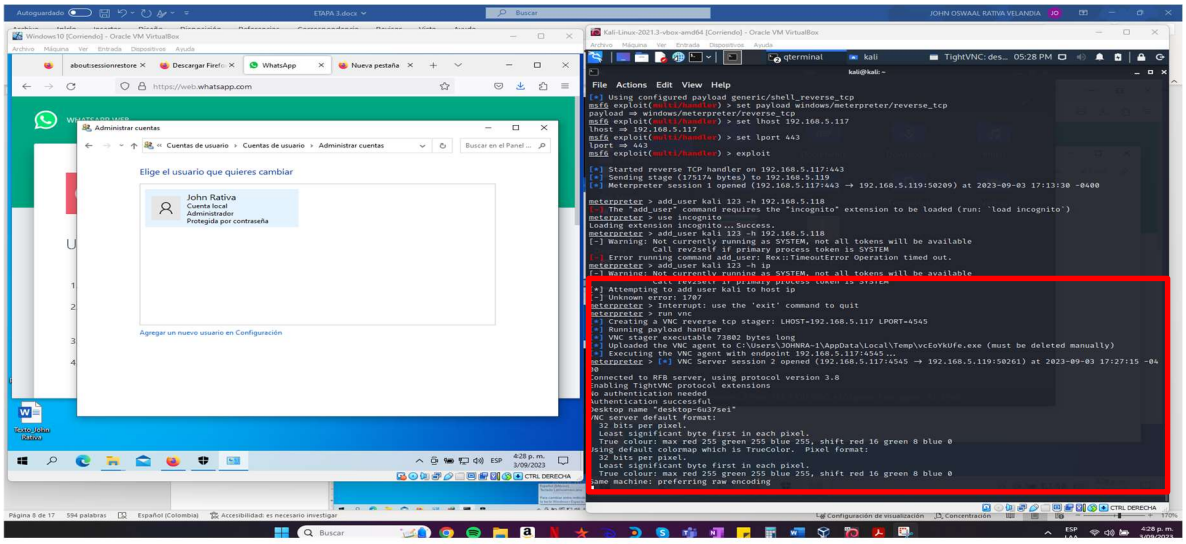
Figura 29 Borrado documentos



Fuente: John Rativa

Adicionalmente, se realiza la ejecución del comando “RUN VNC” el cual nos permite evidenciar en tiempo real lo que realiza el usuario con el fin de obtener más información.

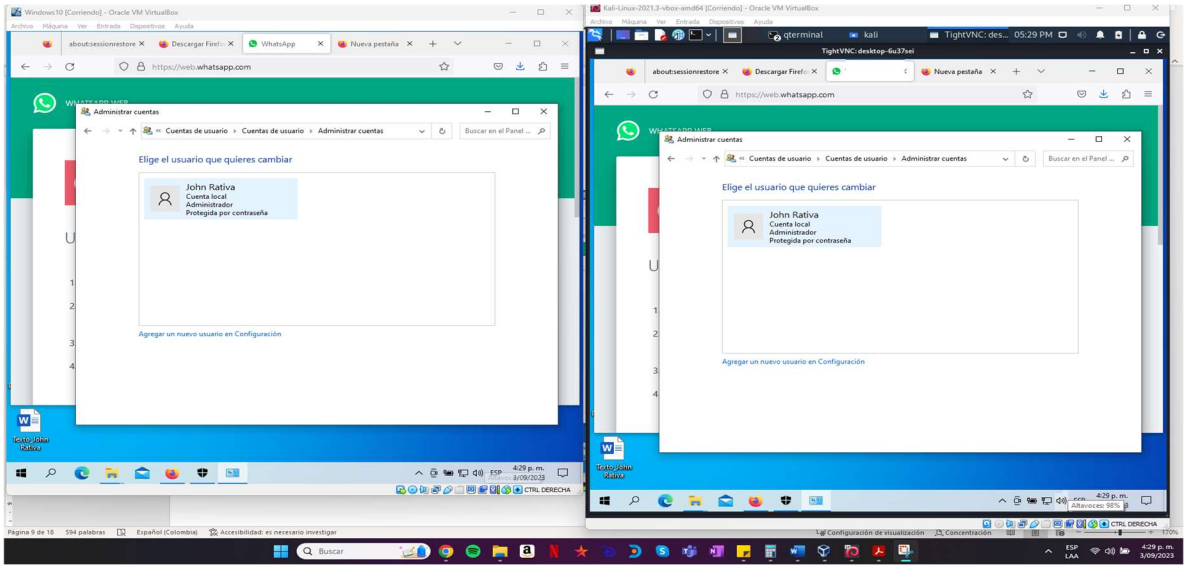
Figura 30 Ejecución VNC



Fuente: John Rativa

De este modo, se puede observar en tiempo real lo realizado por el usuario, logrando captar más información.

Figura 31 conexión exitosa



Fuente: John Rativa

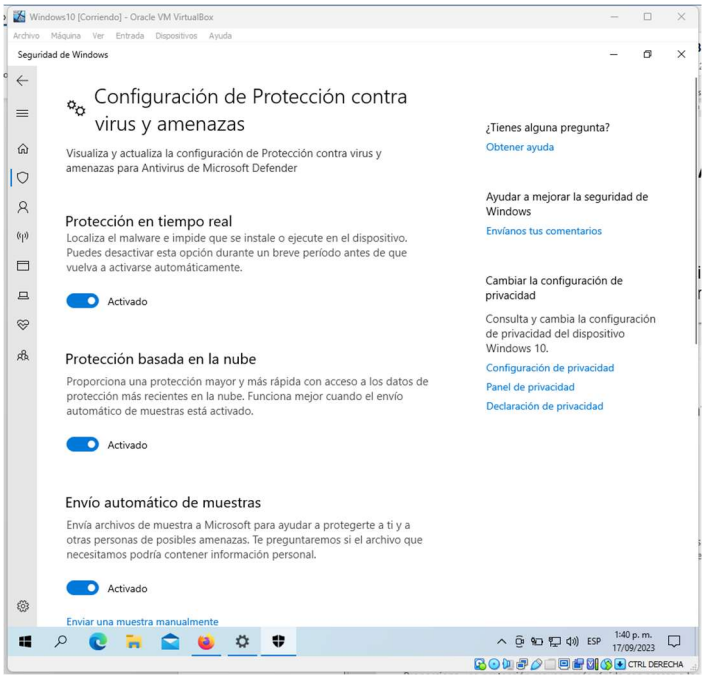
ETAPA 4

LABORATORIO.

Se ha realizado la consulta de diferentes alternativas de hardenización para la máquina afectada, donde, para mejorar la seguridad de la máquina afectada, se realizaron los siguientes pasos:

Se realiza la activación de protección de virus de Windows defender.

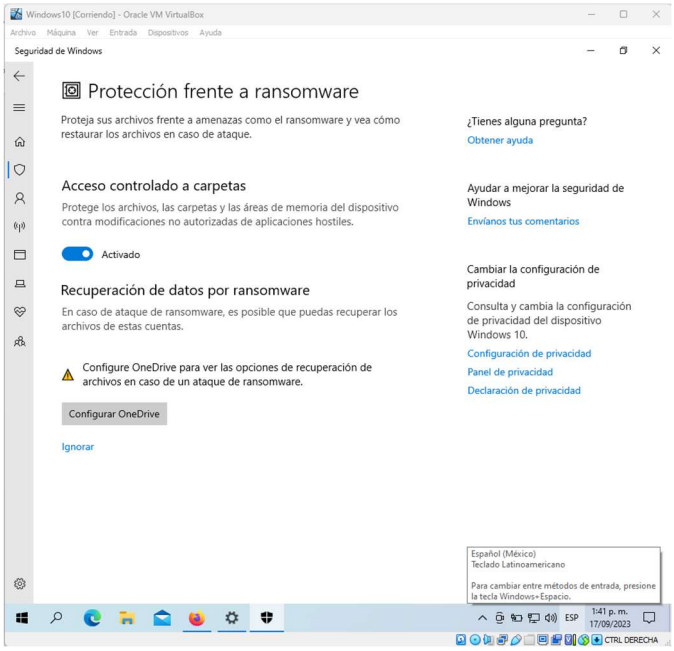
Figura 32 Activación Windows Defender



Fuente: John Rativa

Así como la Activación de protección de Ransomware

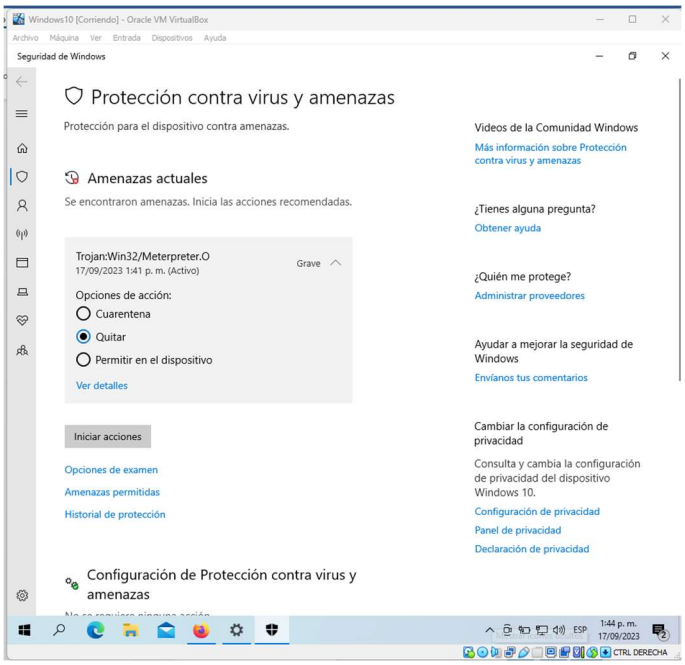
Figura 33 Activación Ransomware



Fuente: John Rativa

Por otra parte, se realiza la eliminación de registros identificados que están afectados por el ataque y que se han identificado en tiempo real.

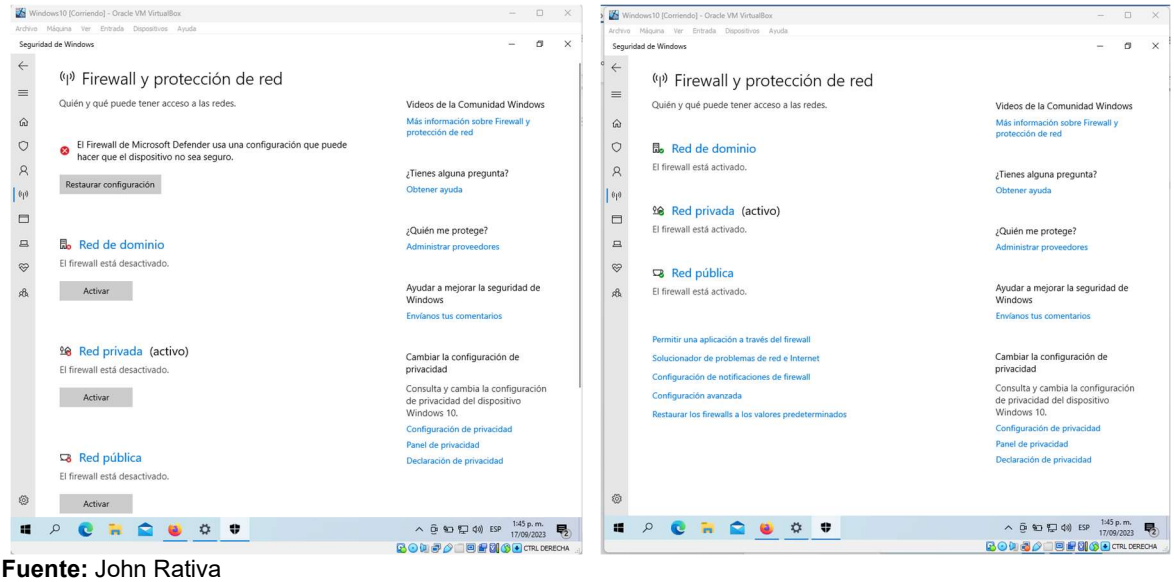
Figura 34 Amenazas actuales equipo



Fuente: John Rativa

También, se realiza la activación de las políticas del firewall.

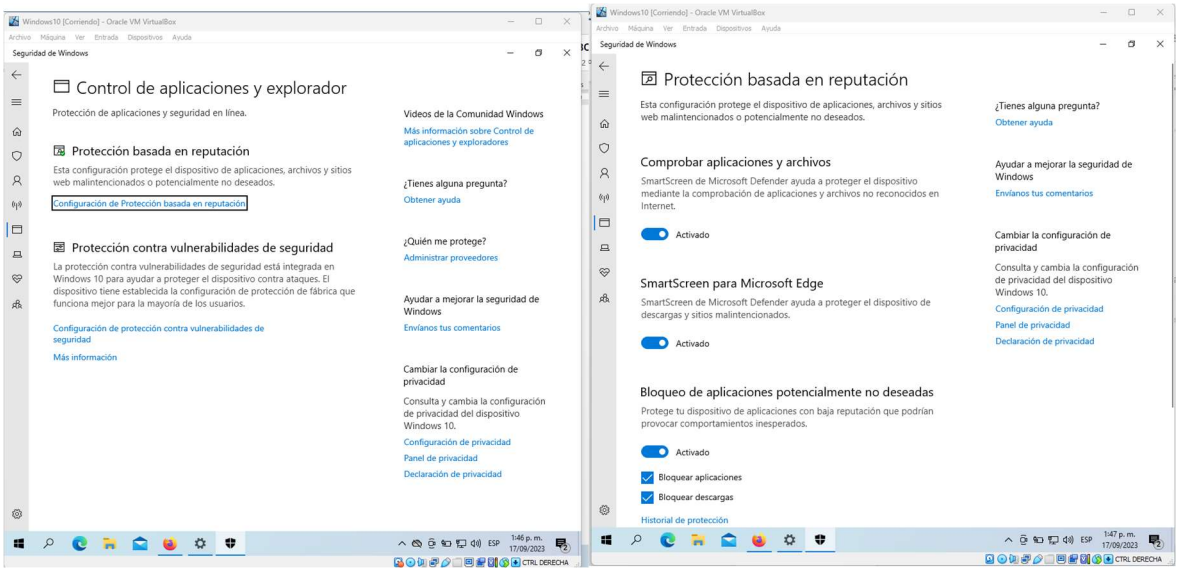
Figura 35 Activación Firewall



Fuente: John Rativa

Se activa el control de aplicaciones y protección basada en reputación, como se muestra a continuación:

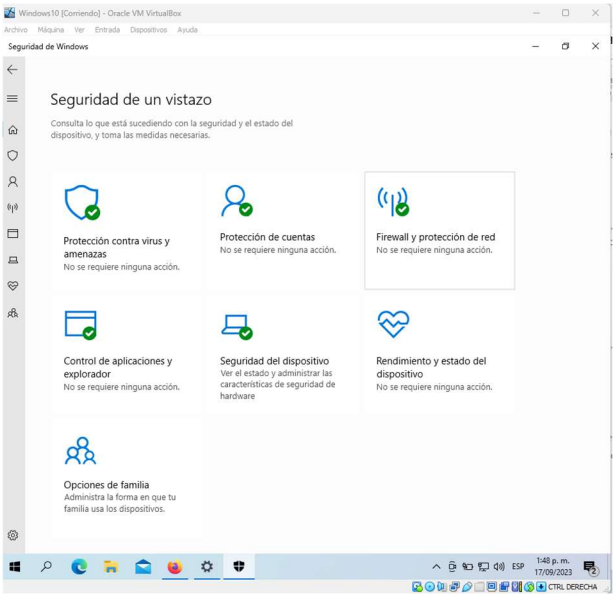
Figura 36 Activación Protección basada en reputación



Fuente: John Rativa

De acuerdo con lo anterior, se confirma que toda la configuración de parámetros mínimos se encuentra correctamente activos.

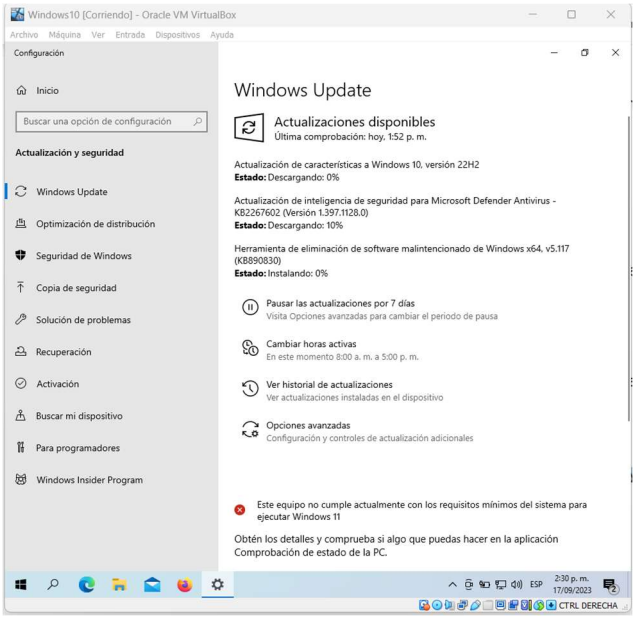
Figura 37 Estado Seguridad principal equipo



Fuente: John Rativa

Por otra parte, se verifica que la máquina cuente con las últimas actualizaciones disponibles, donde, se identifica que cuenta con actualizaciones de seguridad, defender y de características del sistema operativo pendiente.

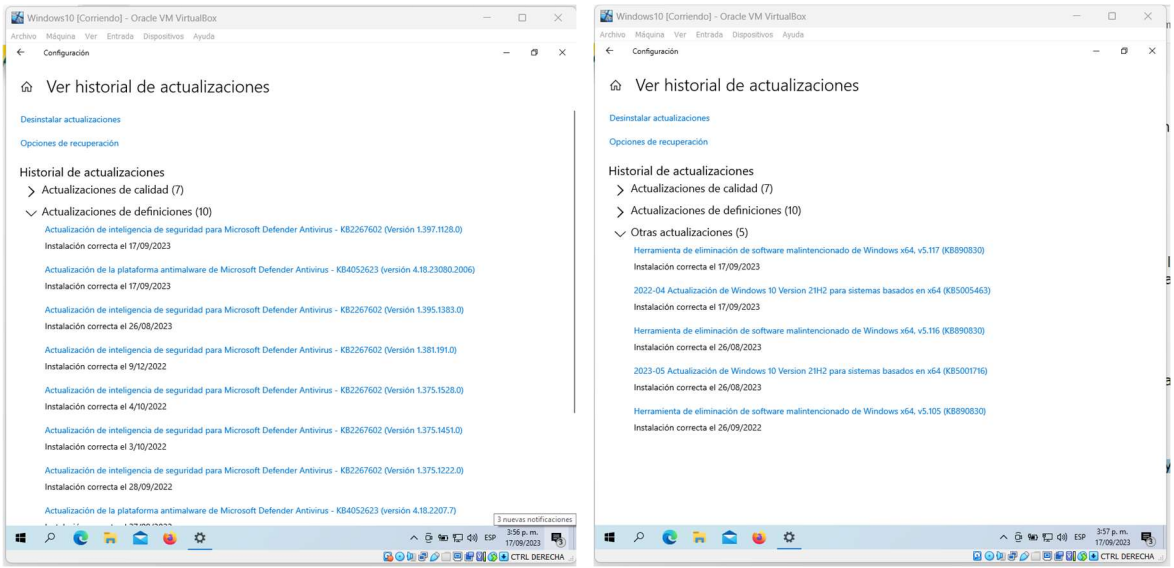
Figura 38 Actualizaciones pendientes



Fuente: John Rativa

Una vez realizado el proceso de verificación de actualizaciones pendientes, se verifica que fueron instaladas correctamente.

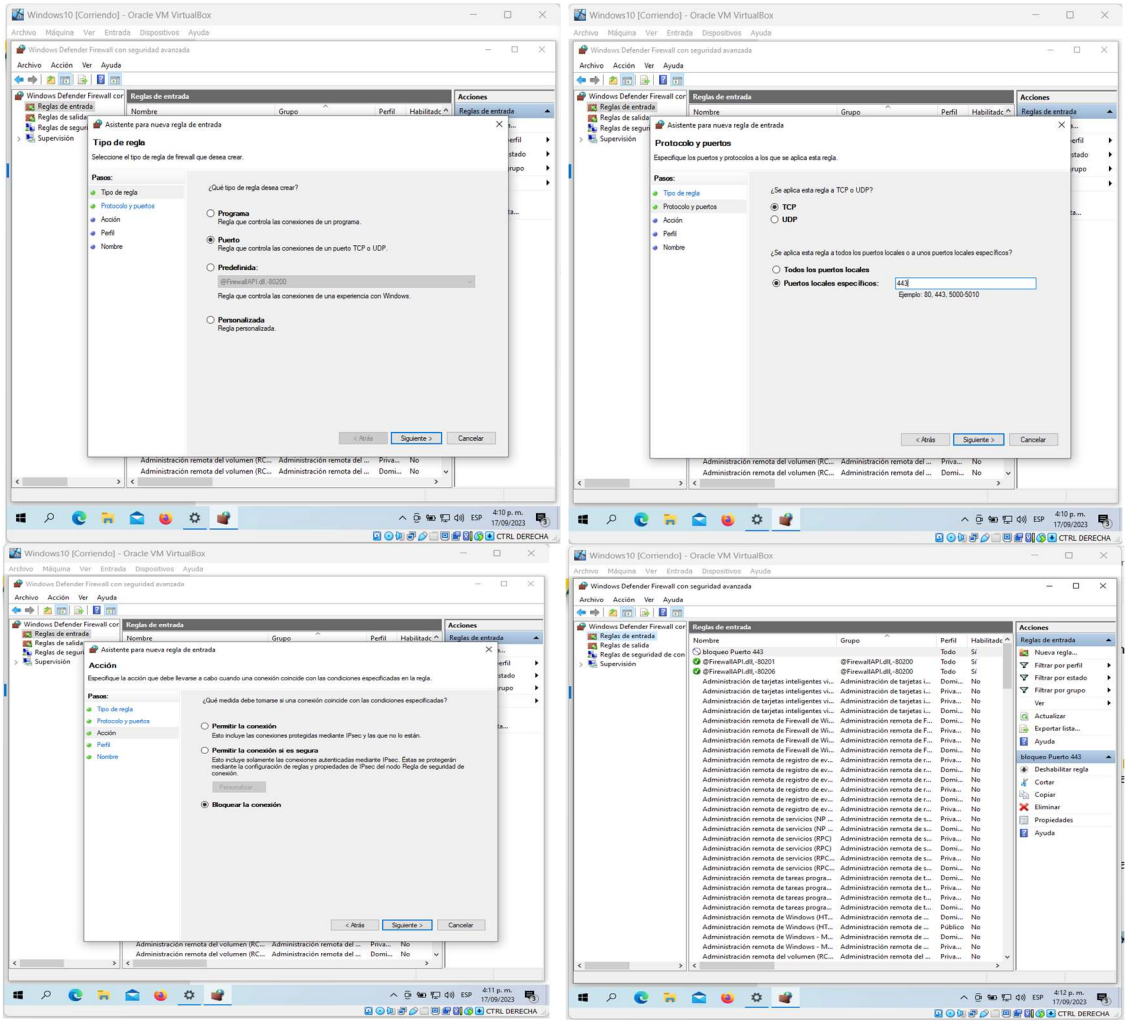
Figura 39 Actualizaciones instaladas



Fuente: John Rativa

Así mismo, se crea una nueva regla en el firewall para no permitir conexiones desde el puerto afectado “443”.

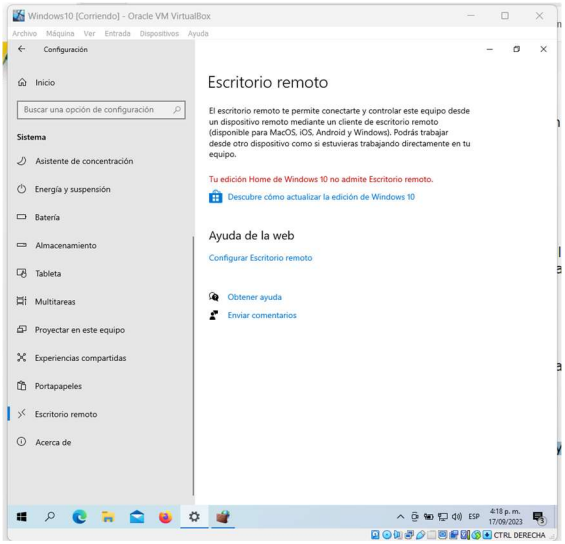
Figura 40 Configuración Regla firewall



Fuente: John Rativa

Por último, se valida que no se cuente habilitada la opción de conexión de escritorio remoto, donde, en este caso, la máquina no lo tiene habilitado de acuerdo con su versión de sistema operativo.

Figura 41 Conexión remota



Fuente: John Rativa

Una vez finalizado el proceso de hardening en el equipo, se realiza el desarrollo de las preguntas del taller, relacionadas a continuación:

PREGUNTA 1

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque?

R:/

Para poder identificar y responder a los ciberataques en tiempo real es fundamental para minimizar los daños y proteger los activos. De este modo, he clasificado las actividades a realizar desde la identificación, hasta posible solución:

Detección de anomalías: podemos utilizar sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear la red en busca de actividades inusuales o patrones de tráfico sospechosos, tráfico malicioso, intentos de acceso no autorizados o actividad inusual del sistema.

Registros de eventos de seguridad: Una vez son identificados los registros de eventos de los sistemas, se realiza análisis de los registros en busca de actividades sospechosas o eventos relacionados con la seguridad de la red. En este caso podemos usar herramientas de gestión de registros como él (SIEM).

Monitoreo del tráfico de red: Se realiza la búsqueda de patrones inusuales en el tráfico de la red, como picos repentinos en el tráfico del servidor o flujos de datos inusuales entre dispositivos. También se realiza la revisión de las conexiones

existentes en el momento, con el fin de identificar conexiones que no se encuentren autorizadas.

Alertas de seguridad: Una vez identificados escenarios específicos de conexión y/o escenarios donde se pueda generar una alerta, se notifica a toda la compañía, informando los sistemas y posible información que puede ser afectada, así como informando su gravedad.

Análisis de malware: si se identifica que el ataque es por parte de malware, se procede a analizar su comportamiento y características para comprender su impacto y cómo eliminarlo.

Eliminación y mitigación: una vez se ha identificado el ataque, se procede a realizar medidas para neutralizar la amenaza y minimizar el daño. Esto puede ser realizando la eliminación del malware, parchear vulnerabilidades, restaurar sistemas a partir de copias de seguridad limpias y actualizar contraseñas en caso de que sea necesario.

Notificaciones: si el incidente involucra datos de clientes, socios o empleados, es necesario notificar al personal interno y externo sobre la información que está siendo afectada.

Recuperación: Hay que tener en cuenta que después de mitigar el ataque, se deben restaurar los sistemas y datos a partir de copias de seguridad limpias y verificadas, asegurando que todo vuelve a su funcionando correcto.

Evaluación de impacto: Finalmente se procede a evaluar el impacto del incidente en la organización, incluidos los costos directos e indirectos, la pérdida de datos y la reputación.

PREGUNTA 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?

R:/

Para el desarrollo de la actividad sobre el ataque presentado en el laboratorio, se realizaron los siguientes pasos:

1. Se activan las configuraciones de protección de virus y amenazas.
2. Se activa la configuración de protección de Ransomware.
3. Se realiza la eliminación de amenazas actuales, incluyendo archivos afectados.
4. Se realiza activación de firewall y configuración de red de dominio.

5. Se activa el control de aplicaciones y protección basada en reputación.
6. Se buscan actualizaciones pendientes y se procede con la respectiva instalación.
7. Se crea reglas de conexión en el firewall para no permitir conexiones desde el puerto donde fue afectada la máquina (443).
8. Se valida que se encuentre desactivada la función de conexión remota.
9. Finalmente, se verifica en el equipo y no se identifican rastros del ataque presentado.

PREGUNTA 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?

R:/

Con el fin de poder hacer un comparativo entre las diferencias entre los equipos, inicialmente, se debe conocer cual es el objetivo principal de cada uno, relacionándolos a continuación:

a. Red Team:

Objetivo principal: Simular ciberataques contra una organización para evaluar sus defensas y descubrir vulnerabilidades.

Rol: Actuar como atacantes éticos para probar y mejorar la seguridad organizacional.
Tiene como objetivo simular ciberataques reales para evaluar las defensas y la preparación de una organización, así como es el encargado de realizar pruebas de penetración y evaluaciones de seguridad. También están encargados de identificar y explotar las debilidades en las defensas de la organización y presentar informes detallados sobre vulnerabilidades y debilidades encontradas.

a. Blue Team:

Objetivo principal: Proteger la infraestructura y los sistemas de la organización frente a ciberamenazas y ataques.

Rol: Implantación y mantenimiento de medidas de seguridad, monitorización de redes y respuesta a incidentes de seguridad de la información.

Son los encargados de implementar medidas de seguridad como firewalls, antivirus y sistemas de detección de intrusos. Así como la supervisión de la red y los sistemas

en busca de actividades sospechosas. Buscan responder a eventos y tomar medidas para mitigar amenazas. Mantener y actualizar políticas y procedimientos de seguridad.

Su foco está en la protección activa, implementación de medidas de seguridad y respuesta en tiempo real ante amenazas.

b. Purple Team:

Objetivo principal: mejorar la cooperación entre el Equipo Rojo y el Equipo Azul y garantizar la eficacia de las pruebas de seguridad de la información.

Rol: Facilitar la comunicación entre los equipos ofensivos (equipo rojo) y defensivos (equipo azul) para mejorar la postura de seguridad.

Facilita la colaboración del equipo rojo y el equipo azul, coordinando ejercicios conjuntos para evaluar la eficacia de la defensa y las capacidades de detección y respuesta. Así como son los encargados de evaluar y documentar las lecciones aprendidas de los ejercicios.

Se centra en los equipos rojo y azul que trabajan juntos para mejorar las capacidades de seguridad de la información de la organización.

c. Equipo de respuesta a incidentes informáticos (CSIRT/CERT):

Objetivo principal: Identificar, gestionar y responder a ciberincidentes reales que afecten a la organización.

Rol: Actuar como primer interviniente ante incidentes de seguridad y tomar medidas para mitigarlos y recuperarse de ellos.

Monitoriza y detecta eventos en tiempo real, además de ser el encargado de investigar casos para comprender su alcance y origen, coordinar la respuesta y recuperación de incidentes, notificar a los interesados y, en algunos casos, a las autoridades pertinentes. Documentar los eventos y las lecciones aprendidas.

Su objetivo principal es gestionar y responder a incidentes cibernéticos reales, incluida la mitigación y recuperación de daños.

Acorde con lo anterior, se puede decir:

Los equipos de respuesta a incidentes cibernéticos se dedican a gestionar incidentes reales, mientras que el Purple Team facilitan la colaboración entre el Red Team y el Blue Team para mejorar la seguridad.

Los equipos Red Team son los encargados de simular ataques contra la organización, para que finalmente el equipo Blue Team se centre en defensas activas y defensas de infraestructura. Todos estos grupos desempeñan un papel importante en la estrategia general de ciberseguridad de una organización realizando cada actividad dentro de su alcance.

PREGUNTA 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.

R:/

El Centro para la Seguridad de Internet (CIS) tiene como papel importante proporcionar recursos y herramientas esenciales para mejorar la seguridad organizacional y respaldar las operaciones del Blue Team, donde, entre Las principales funciones del CIS en relación con los Equipos Azules incluyen:

El CIS es conocido por desarrollar y mantener "Controles CIS" (anteriormente "Controles de seguridad críticos SANS"), siendo un conjunto ampliamente reconocido de pautas y mejores prácticas de ciberseguridad. Las directrices ayudan a las organizaciones a identificar y priorizar acciones específicas para mejorar la seguridad. Los equipos de Blue Team utilizan estas instrucciones para fortalecer sus defensas.

La CIS proporciona herramientas y recursos gratuitos para los Blue Team, incluyendo herramientas de evaluación de seguridad, políticas de seguridad y plantillas de configuración, guías de implementación y más para ayudarlo a implementar funciones de seguridad efectivas.

También, proporciona herramientas de evaluación y evaluaciones comparativas que permiten a las organizaciones medir su postura de seguridad y compararla con los estándares de la industria para ayudar a los equipos de blue Team a identificar áreas de mejora y priorizar sus esfuerzos.

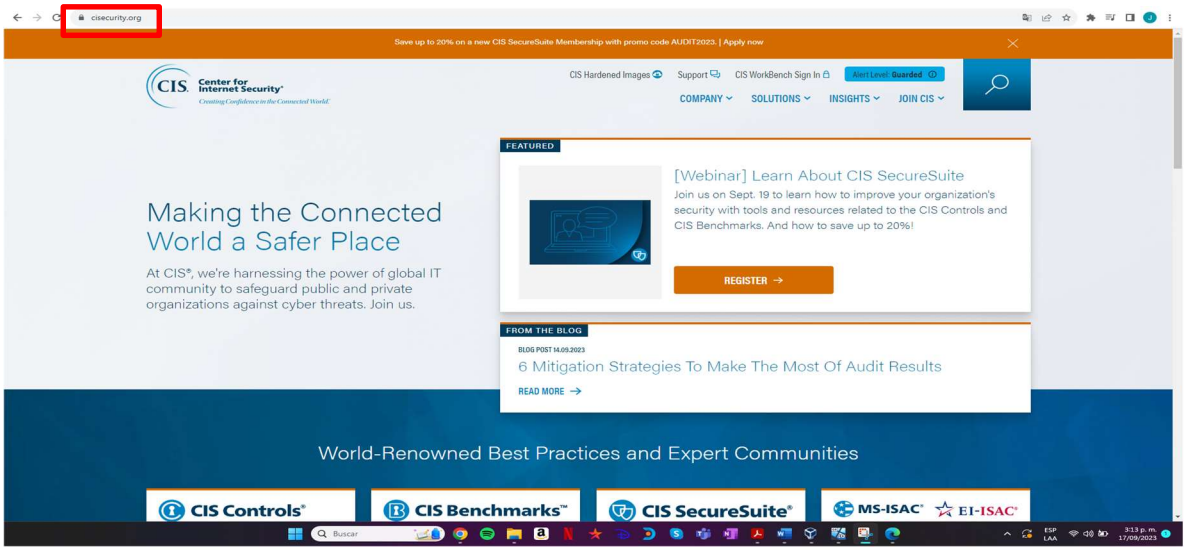
Por otra parte, proporciona recursos relacionados con programas de concientización sobre seguridad cibernética y respuesta a emergencias con el fin de ayudar a los equipos de Blue Team a estar preparados para detectar, responder y mitigar violaciones de seguridad y capacitar a los empleados sobre buenas prácticas de seguridad.

Manual CIS

1. Ir al sitio web del CIS:

Visite el sitio web oficial del Centro para la Seguridad de Internet en https://www.cisecurity.org/. Este sitio web es la principal fuente de información y recursos del CIS.

Figura 42 Cis página principal

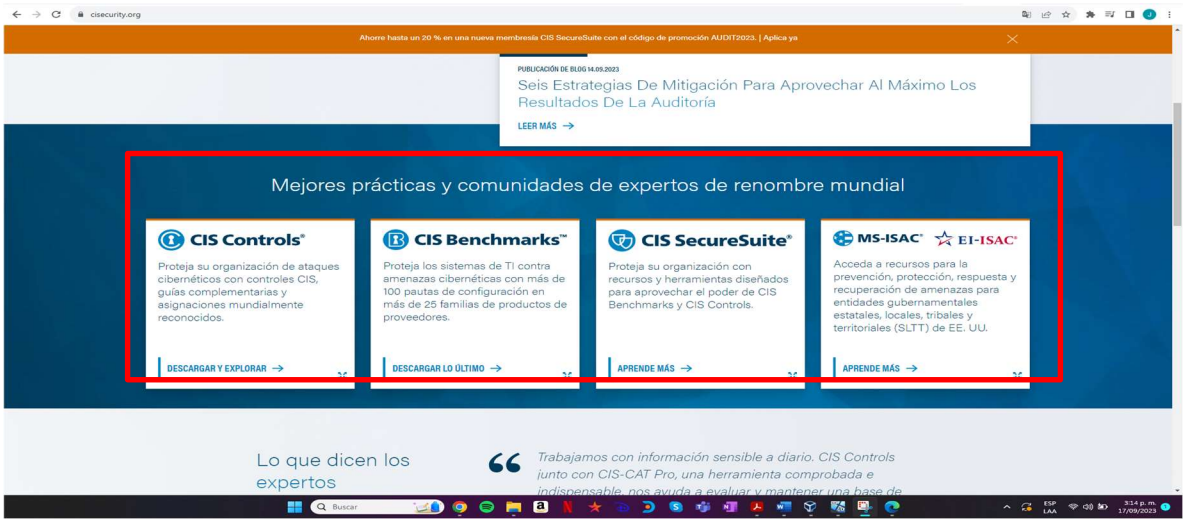


Fuente: John Rativa

2. Consulte los recursos:

Navegue por el sitio web de CIS para explorar los recursos disponibles. Estos recursos suelen dividirse en categorías como "Controles CIS", "Parámetros", "Herramientas", "Capacitación" y "Documentación". Aquí hay algunas áreas importantes a considerar:

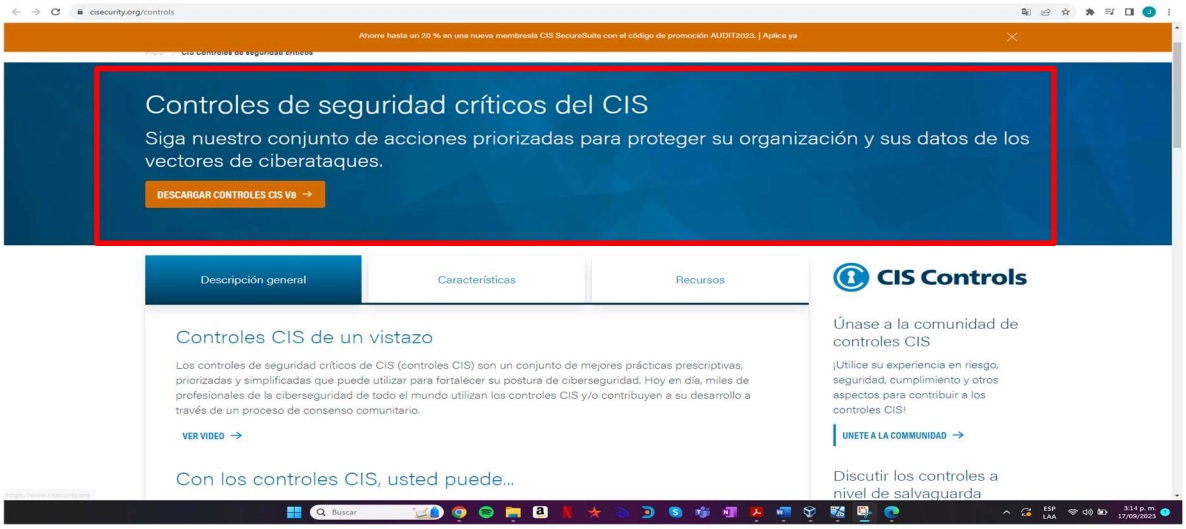
Figura 43 Opciones CIS



Fuente: John Rativa

3. Ingresar en la opción que se desea consultar, sea la opción de controles o otra de las disponibles.

Figura 44 Opciones CIS

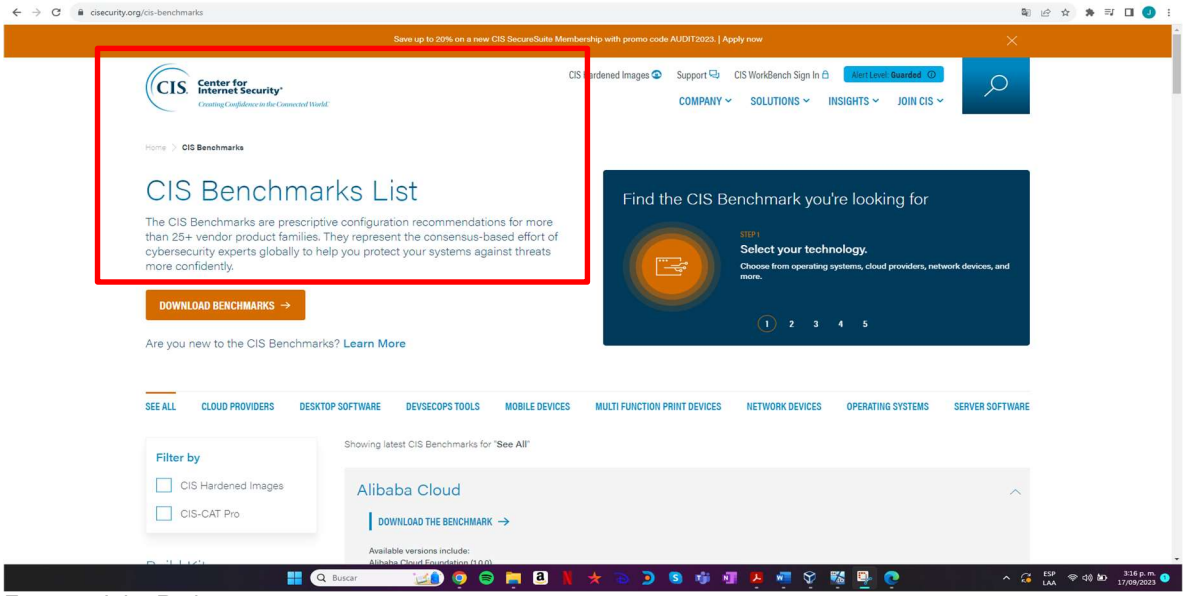


Fuente: John Rativa

4. Ingreso a Opciones disponibles.

En esta opción, encontramos las pautas esenciales para mejorar la ciberseguridad. Donde se puede descargar documentación detallada que describe cada control y su implementación.

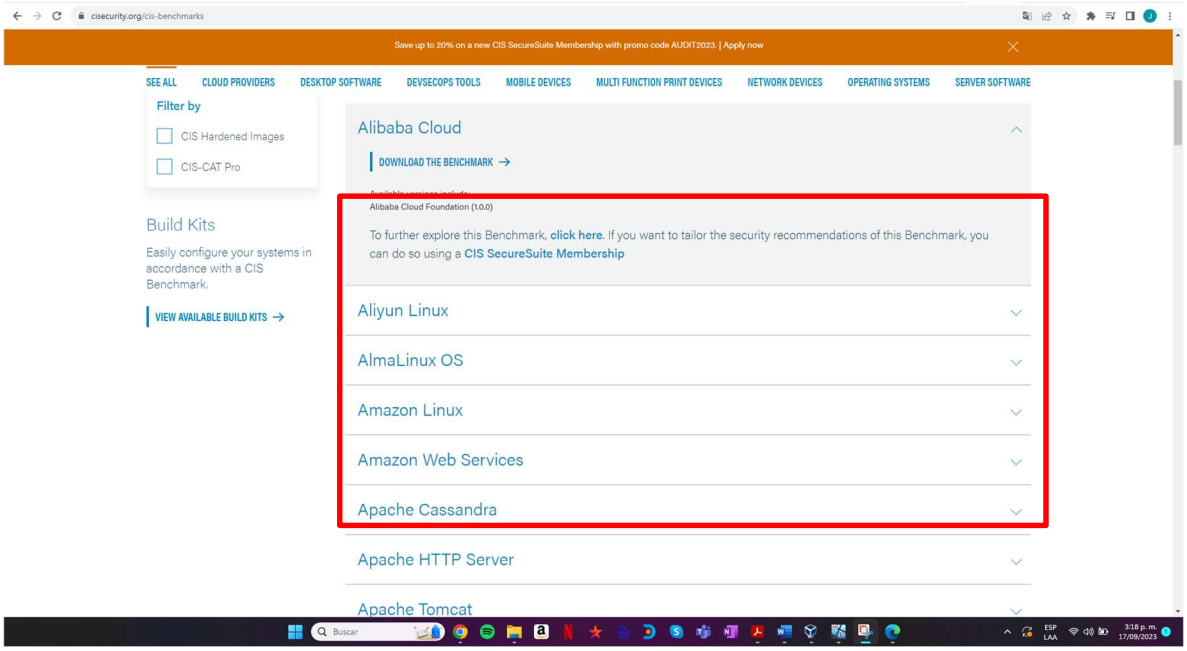
Figura 45 Pautas CIS



Fuente: John Rativa

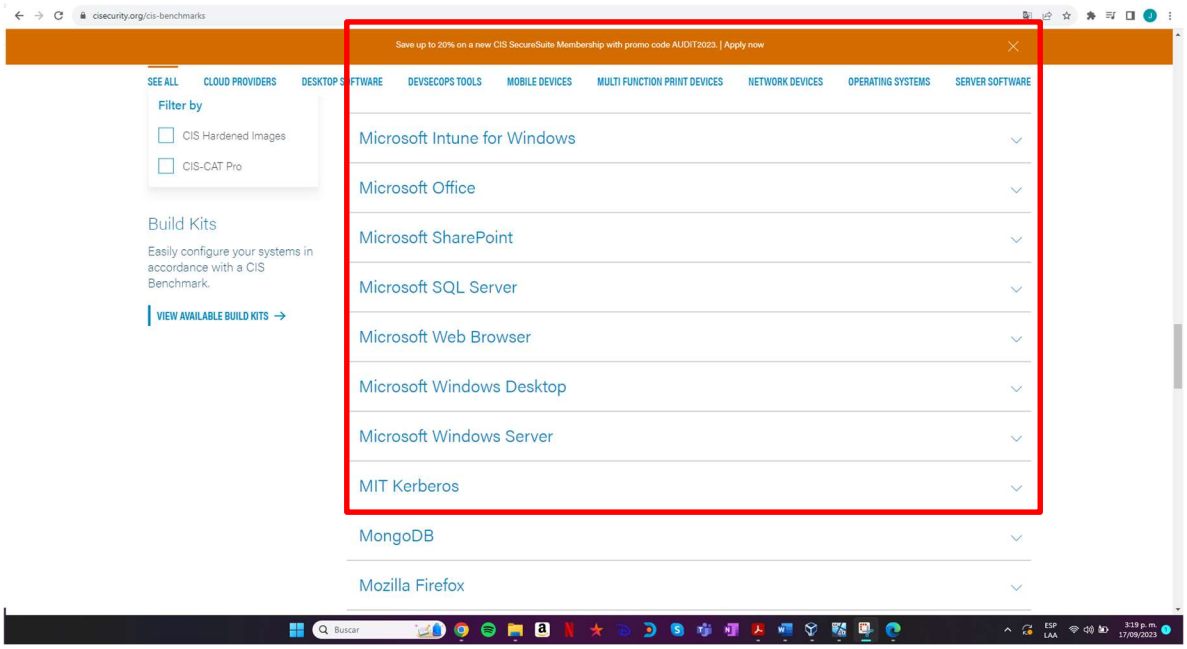
5. Seleccionar el sistema Operativo, o las opciones a las cuales desea consultar:

Figura 46 Listado Sistemas Operativos CIS 1



Fuente: John Rativa

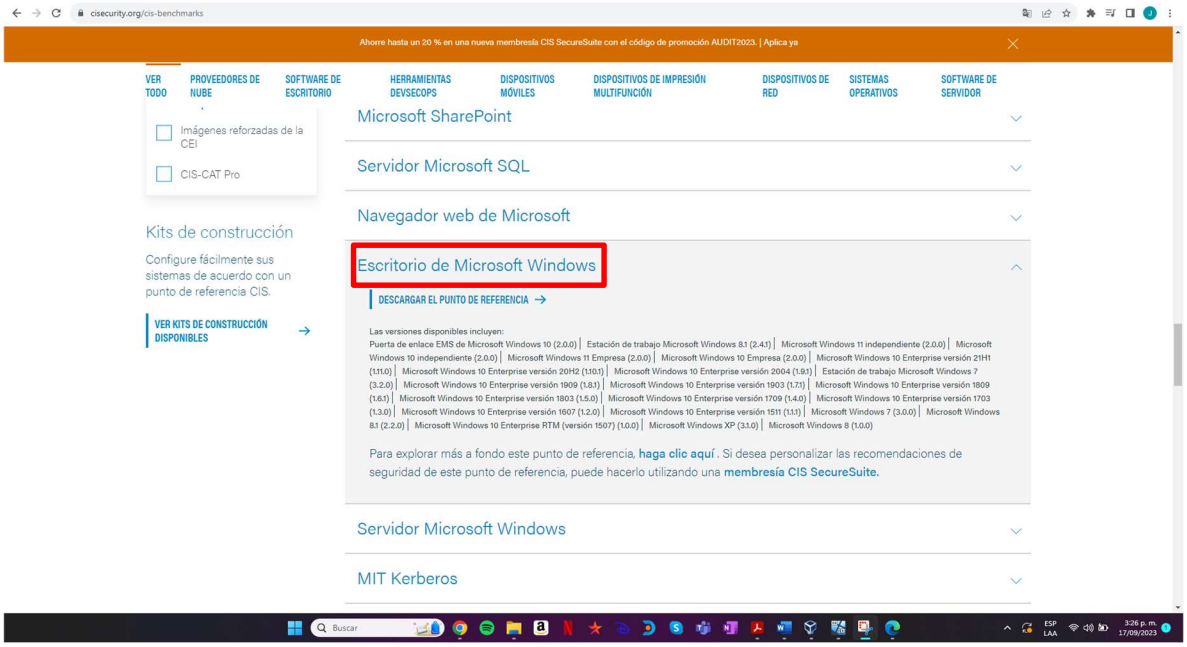
Figura 47 Listado Sistemas Operativos CIS 2



Fuente: John Rativa

6. Se selecciona el sistema Operativo y se ingresa a descargar la información de referencia.

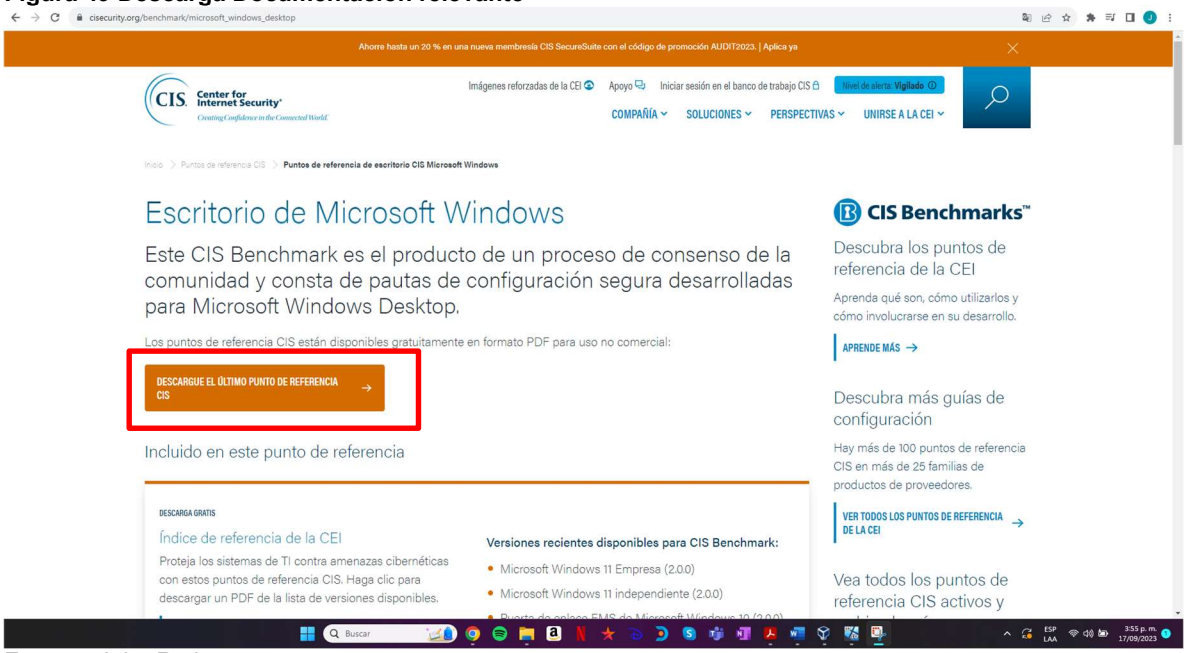
Figura 48 Ingreso Sistema Operativo CIS



Fuente: John Rativa

7. Se ingresa a descarga de la documentación disponible.

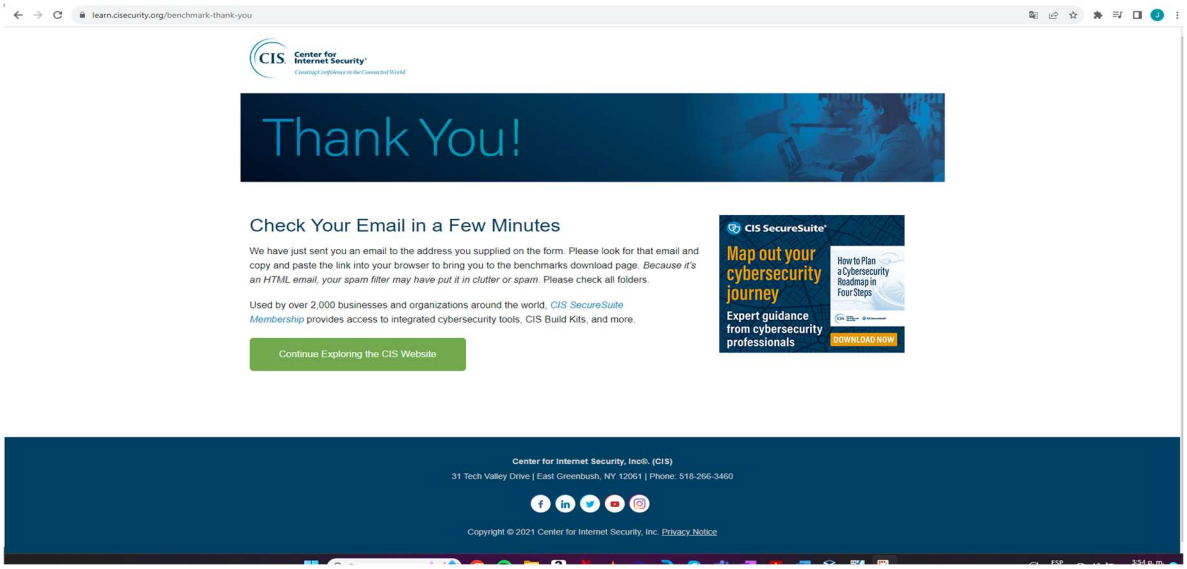
Figura 49 Descarga Documentación relevante



Fuente: John Rativa

8. Se debe realizar el diligenciamiento de formato de datos para acceder a la descarga de la información.

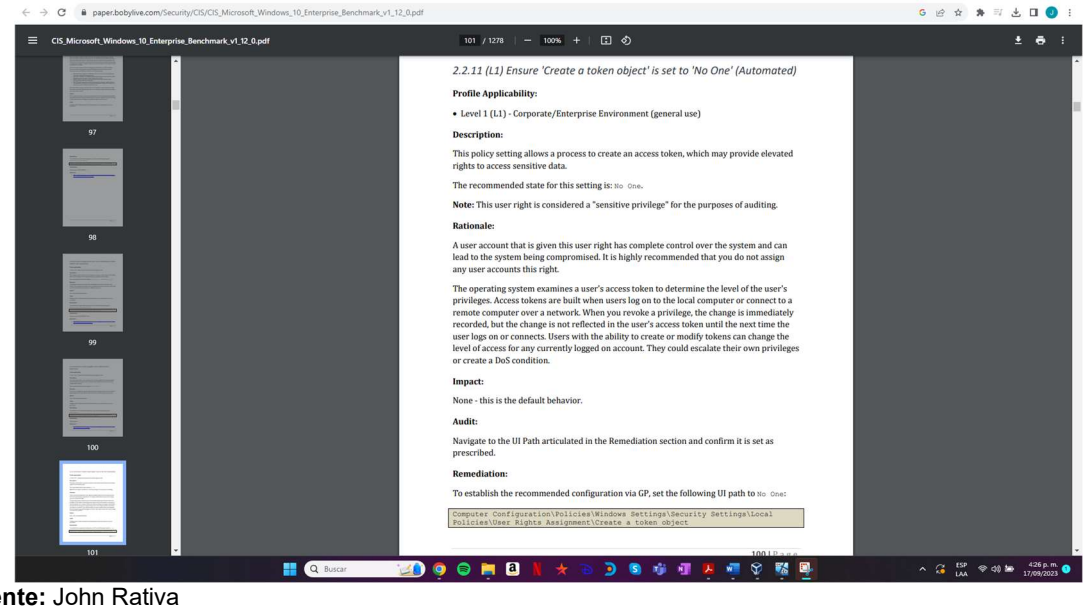
Figura 50 Descarga Aprobada



Fuente: John Rativa

9. Una vez se recibe la información, se cuenta con información guía para los equipos de Blue Team, sobre el desarrollo de procesos, con notas, impacto y remediación de diferentes escenarios.

Figura 51 Documento CIS



Fuente: John Rativa

PREGUNTA 5

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

R:/

Para el desarrollo de las diferencias entre el SIEM y el XDR, se realiza la evaluación de diferentes aspectos, relacionados a continuación:

Tabla 1 Comparación SIEM y XDR

Ítem	SIEM	XDR
Definición	Una plataforma de gestión de seguridad de la información que recopila correlaciona y analiza registros y eventos de seguridad de múltiples fuentes.	Una plataforma de seguridad que va más allá de SIEM, ya que integra capacidades de detección, respuesta y análisis avanzados para amenazas.
Alcance	Se centra en la gestión de eventos y la generación de informes basados en registros de seguridad.	Amplía su alcance más allá de los registros para incluir fuentes de datos diversificadas, como registros, puntos finales, redes y más.
Fuentes de datos	Principalmente se basa en registros de seguridad de sistemas, aplicaciones y redes.	Puede integrar una variedad de fuentes de datos, incluidos registros, endpoints, tráfico de red, amenazas conocidas y comportamiento anómalo.
Detección de amenazas	Limitado a la correlación de eventos y reglas predefinidas para detectar amenazas conocidas.	Utiliza análisis avanzados y aprendizaje automático para detectar amenazas conocidas y desconocidas, así como patrones de actividad maliciosa.
Respuesta a amenazas	Por lo general, proporciona alertas y notificaciones para que los equipos de seguridad tomen medidas.	Ofrece capacidades de respuesta automatizada y orquestación para mitigar amenazas de manera más rápida y eficiente.
Análisis de amenazas	Ofrece análisis limitados, principalmente basados en la correlación de eventos y reglas.	Proporciona análisis avanzados de amenazas, incluida la investigación de incidentes, la

Ítem	SIEM	XDR
		trazabilidad y el análisis forense.
Visibilidad	Ofrece visibilidad en tiempo real y análisis retrospectivo de eventos de seguridad.	Proporciona una visibilidad más amplia y profunda en toda la infraestructura de seguridad y permite una búsqueda exhaustiva y análisis.
Automatización	Limitada en términos de automatización de respuesta a amenazas.	Incorpora automatización avanzada para responder a amenazas y realizar acciones de remediación de manera más rápida y precisa.
Escalabilidad	A menudo, es menos escalable en comparación con las soluciones XDR.	Diseñado para ser altamente escalable y adaptable a entornos de gran envergadura.
Madurez	Una tecnología de seguridad consolidada, pero con limitaciones en la detección avanzada de amenazas.	Una tecnología emergente que aborda las limitaciones de SIEM y evoluciona con las amenazas modernas.

Fuente: John Rativa

PREGUNTA 6

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

R:/

A Continuación, se relacionan las herramientas para la detección de ataques informáticos.

Snort:

Es un sistema de detección de intrusiones (IDS) y un sistema de prevención de intrusiones (IPS) que monitorea el tráfico de red en busca de patrones y firmas de ataques conocidos. Se puede configurar para generar alertas en tiempo real o tomar acciones proactivas.

Suricata:

Es un motor de detección de amenazas en línea de código abierto. Detecta y registra actividad sospechosa en el tráfico de la red y es altamente configurable y escalable.

Bro (ahora Zeek):

Es una plataforma de análisis de tráfico de red que se utiliza para registrar y analizar el tráfico de red para detectar comportamientos anómalos y patrones de ataque. Esto puede ayudar a detectar intrusiones y actividades sospechosas.

Fail2Ban:

Es una herramienta utilizada para prevenir la fuerza bruta y otros ataques basados en patrones en servicios como SSH, FTP o servidores web. Bloquea automáticamente las direcciones IP del atacante después de una cierta cantidad de intentos fallidos.

Snorby:

Es una interfaz web que se utiliza para administrar y ver registros y alertas generadas por Snort y Suricata. Facilita la revisión y análisis de eventos de seguridad en un ambiente más amigable.

ETAPA 5

PRETUNTA 1

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

R:/
Reunir un Blue Team, un Red Team y un Purple Team al mismo tiempo en una organización puede mejorar significativamente la seguridad cibernética. Esta integración fomenta la colaboración, la evaluación continua y el fortalecimiento de las ciberdefensas de una organización de varias maneras:

Mejor comunicación: la colaboración entre estos equipos mejora la comunicación interna. El Blue Team y el Red Team pueden trabajar juntos de manera más efectiva y compartir información sobre amenazas, vulnerabilidades y medidas de seguridad.

Detección de vulnerabilidades más eficaz: los equipos de Red Team pueden identificar vulnerabilidades en la infraestructura de TI de una organización mediante pruebas de penetración realistas. Los equipos de blue Team pueden utilizar estas observaciones para fortalecer las defensas y cerrar brechas.

Pruebas más realistas: la colaboración entre el Red Team y el Blue Team permite pruebas más realistas. Los Equipos de Red Team pueden adaptar sus tácticas a las

defensas existentes, ayudando a evaluar las capacidades de detección y respuesta del Blue Team.

Mejora Continua: El Equipo de Purple Team es responsable de facilitar la colaboración y las evaluaciones conjuntas. Promueve una cultura de mejora continua de la ciberseguridad dentro de la organización.

Evaluación de seguridad integral: la integración de estos grupos permite una evaluación de seguridad integral. Además de las medidas de seguridad técnicas, también se evalúan los procesos, los métodos operativos y la formación personal.

Capacitación y desarrollo: los equipos de Blue Team pueden aprender de las tácticas y técnicas de los Equipos de Red Team. Esto mejora la capacidad del Blue Team para detectar y responder a amenazas cibernéticas.

Preparación para incidentes: al simular ataques del mundo real y evaluar una respuesta del Blue Team, la organización está mejor preparada para incidentes cibernéticos reales. Esto acorta el tiempo de respuesta y minimiza el impacto de situaciones peligrosas.

Alineación con los objetivos comerciales: la integración de estos equipos ayuda a alinear la ciberseguridad con los objetivos comerciales de la organización. Las inversiones en seguridad se pueden priorizar en función de los riesgos y amenazas identificados.

Cumplimiento y regulaciones: ayuda a cumplir con los requisitos y regulaciones de ciberseguridad, garantizando que las defensas estén en línea con las mejores prácticas y los estándares de la industria.

Ahorro de costos a largo plazo: al identificar y mitigar vulnerabilidades de manera proactiva, puede reducir los costos asociados con la respuesta a incidentes y la recuperación después de una violación de seguridad.

En conclusión, la integración de Blue Team, Red Team y Purple Team contribuye a una estrategia de ciberseguridad más eficaz y adaptable. Facilita la detección temprana de riesgos, la mitigación proactiva de amenazas y la mejora continua de las defensas de una organización, lo cual es esencial en un entorno cibernético en constante evolución.

PREGUNTA 2

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

R:/
El buen uso de configuraciones de seguridad en equipos de cómputo es esencial para proteger la integridad, confidencialidad y disponibilidad de datos y sistemas. Configuraciones adecuadas, como contraseñas sólidas, actualizaciones regulares, firewall y software de seguridad, pueden prevenir amenazas cibernéticas y ataques. La conciencia y educación sobre seguridad son clave para mantener la protección.

Los equipos de seguridad de las compañías desempeñan roles esenciales en la protección de las organizaciones contra las amenazas cibernéticas, y su colaboración y la adopción de mejores prácticas son vitales para mantener la seguridad en un entorno digital cada vez más complejo y peligroso.

Realizar un adecuado hardening es esencial para fortalecer la seguridad de un sistema informático o red, proteger los datos y cumplir con las regulaciones. Sin embargo, es importante recordar que la seguridad es un proceso continuo y que las amenazas cambian con el tiempo, por lo que el hardening debe ser parte de una estrategia de seguridad integral.

El buen uso de configuraciones de seguridad en equipos de cómputo es esencial para proteger la integridad, confidencialidad y disponibilidad de datos y sistemas. Configuraciones adecuadas, como contraseñas sólidas, actualizaciones regulares, firewall y software de seguridad, pueden prevenir amenazas cibernéticas y ataques. La conciencia y educación sobre seguridad son clave para mantener la protección.

RECOMENDACIONES

De acuerdo con el escenario presentado y la información recopilada en cada una de las fases, debemos tener en cuenta diferentes recomendaciones para estar atentos ante un ataque, o acciones a generar posterior a estos:

Responde de inmediato:
Identificar y aislar la fuente del ataque implica detener cualquier actividad maliciosa y desconectar los sistemas comprometidos de la red para evitar que el atacante siga operando en ellos.

Notifica a las partes pertinentes:
Informa a los responsables de seguridad de la organización, incluyendo al equipo de respuesta a incidentes de seguridad (CSIRT) si se tiene uno. También debes considerar notificar a las autoridades legales y reguladoras pertinentes, como las agencias de protección de datos o las fuerzas del orden si se trata de un ataque grave.

Preserva la evidencia:
No modifiques ni elimines ningún dato relacionado con el ataque. Esto incluye registros de actividad, registros de firewall, correos electrónicos de phishing,

archivos maliciosos, etc. Preservar la evidencia es esencial para investigaciones y posibles acciones legales.

Recopila información:
Determina qué tipo de ataque ocurrió (por ejemplo, malware, phishing, ataque de denegación de servicio, etc.). Recopila información sobre cómo se llevó a cabo y qué sistemas se vieron afectados. Esto ayudará en la investigación y la mitigación.

Aísla y restaura sistemas:
Aísla los sistemas comprometidos para evitar la propagación del ataque a otras partes de la red. Luego, restaura los sistemas afectados utilizando copias de seguridad verificadas y libres de malware.

Realiza un análisis de causa raíz:
Investiga cómo se llevó a cabo el ataque y por qué los sistemas de seguridad existentes no lo detectaron o impidieron. Esto implica identificar las debilidades en la infraestructura y las políticas de seguridad.

Aplica medidas de hardening:
Fortalece la seguridad de tus sistemas mediante la aplicación de parches y actualizaciones de seguridad, el endurecimiento de la configuración de sistemas y aplicaciones, la gestión de contraseñas más seguras, la implementación de políticas de acceso y privilegios adecuadas, entre otros.

Capacita al personal:
Proporciona capacitación en concienciación sobre seguridad cibernética a los empleados para que sean conscientes de las amenazas y sepan cómo identificar y reportar posibles ataques, como el phishing.

Mejora la detección y respuesta:
Implementa sistemas de detección de intrusiones (IDS) y sistemas de información y eventos de seguridad (SIEM) para monitorear la actividad en tiempo real y responder rápidamente a incidentes. Establece procedimientos de respuesta a incidentes claros para guiar al personal en caso de futuros ataques.

Realiza pruebas de penetración:
Contrata a expertos en seguridad para realizar pruebas de penetración que evalúen la resistencia de tus sistemas y aplicaciones a ataques simulados. Esto ayuda a identificar posibles vulnerabilidades.

Mantén la comunicación:
Comunica de manera regular y transparente el progreso de la respuesta al incidente y el proceso de fortalecimiento de la seguridad a las partes interesadas, como la alta dirección, los empleados y los clientes si es necesario.

Cumple con las regulaciones y leyes aplicables:
Asegúrate de cumplir con las obligaciones legales y reglamentarias relacionadas con la notificación de brechas de seguridad y la protección de datos, especialmente si se vieron comprometidos datos de clientes o empleados.

Monitorea continuamente:
Mantén un monitoreo constante de la seguridad de tus sistemas y redes utilizando herramientas de seguridad cibernética para detectar posibles amenazas en tiempo real.

Documenta el incidente y las acciones tomadas:
Lleva un registro detallado de todas las actividades relacionadas con el incidente, incluyendo la respuesta, las medidas de hardening implementadas y cualquier hallazgo de la investigación. Esto es importante para futuras referencias y auditorías.

Realiza auditorías y evaluaciones periódicas:
Programa auditorías regulares de seguridad para evaluar el cumplimiento de las políticas y procedimientos de seguridad y asegurarte de que las medidas de hardening sigan siendo efectivas.

CONCLUSIONES

- Los ataques de robo de información representan una seria amenaza para la privacidad, la seguridad y la integridad de los datos en un sistema. Pueden tener consecuencias devastadoras, incluyendo la pérdida de datos, la exposición de información confidencial y daños financieros, lo que subraya la importancia de contar con medidas sólidas de seguridad cibernética para prevenirlos y mitigar sus impactos.

- La inversión en ciberseguridad ayuda a proteger los activos más valiosos de una organización, como datos confidenciales, propiedad intelectual y sistemas críticos. La pérdida o el robo de estos activos podría tener un impacto devastador en la empresa.

- La inversión en ciberseguridad es una medida proactiva y estratégica que ayuda a las organizaciones a protegerse contra las crecientes amenazas cibernéticas y a cumplir con las expectativas de sus partes interesadas. Es fundamental para la continuidad del negocio, la reputación y la competitividad en un entorno digital cada vez más complejo y peligroso.

- Garantizar la seguridad de los equipos informáticos es de vital importancia para salvaguardar la integridad, confidencialidad y disponibilidad de los datos y sistemas. Para lograrlo, es imprescindible implementar configuraciones adecuadas, como contraseñas robustas, mantener actualizaciones periódicas, hacer uso de firewalls y utilizar software de seguridad.

- Los equipos encargados de la seguridad en las organizaciones desempeñan roles cruciales en la defensa contra las amenazas cibernéticas. La colaboración entre estos equipos y la adopción de las mejores prácticas son esenciales para preservar la seguridad en un entorno digital en constante evolución y cada vez más peligroso.

- La realización de un adecuado proceso de fortificación (hardening) es esencial para reforzar la seguridad de un sistema informático o una red, asegurando la protección de los datos y el cumplimiento de las regulaciones pertinentes. Sin embargo, es importante tener en mente que la seguridad es un proceso continuo, y las amenazas evolucionan con el tiempo, por lo que el proceso de fortificación debe ser parte integral de una estrategia global de seguridad.

- Los equipos de seguridad de las compañías desempeñan roles esenciales en la protección de las organizaciones contra las amenazas cibernéticas, y su colaboración y la adopción de mejores prácticas son vitales para mantener la seguridad en un entorno digital cada vez más complejo y peligroso.

- Realizar un adecuado hardening es esencial para fortalecer la seguridad de un sistema informático o red, proteger los datos y cumplir con las regulaciones. Sin embargo, es importante recordar que la seguridad es un proceso continuo y que las amenazas cambian con el tiempo, por lo que el hardening debe ser parte de una estrategia de seguridad integral.

- El buen uso de configuraciones de seguridad en equipos de cómputo es esencial para proteger la integridad, confidencialidad y disponibilidad de datos y sistemas. Configuraciones adecuadas, como contraseñas sólidas, actualizaciones regulares, firewall y software de seguridad, pueden prevenir amenazas cibernéticas y ataques. La conciencia y educación sobre seguridad son clave para mantener la protección.

BIBLIOGRAFIA

ADSLZone. CÓMO ABRIR y cerrar puertos en el firewall de Windows 10 [en Línea]. [Consultado el 15, septiembre, 2023]. Disponible en Internet: https://www.adslzone.net/esenciales/windows-10/abrir-puertos-firewall/

Bidaidea. ¿CUÁL SON La 5 Fases Del Pentesting? – Ciberseguridad. [en Línea]. [Consultado el 10, agosto, 2023]. Disponible en Internet: https://ciberseguridadbidaidea.com/fases-del-pentesting

Blogthinkbig.com. Así puedes eliminar archivos de Windows por más que se resistan. (s.f.). [en Línea]. [Consultado el 18, septiembre, 2023]. Disponible en Internet: https://www.cisecurity.org/

CalCom. 10 ETAPAS DE HARDENING DE WINDOWS PARA MEJORAR LA RESILIENCIA CIBERNÉTICA | CalCom [en Línea]. [Consultado el 18, septiembre, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Carbide. SECURITY BEST Practices for Your Windows 10 Computer | Carbide [en Línea]. (25, septiembre, 2023). [Consultado el 29, septiembre, 2023]. Disponible en Internet: https://carbidesecure.com/resources/security-best-practices-hardening-windows-10/

Copnia. CÓDIGO DE ética | Copnia [en Línea]. (20, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Dirección de Impuestos y Aduanas Nacionales. - DIAN PRENSA Comunicado de Prensa No. 024 [en Línea]. (20, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: https://www.dian.gov.co/Prensa/Paginas/NG-Comunicado-de-Prensa-024-2023.aspx

DominioGeek. CÓMO comprobar, abrir y cerrar puertos en Windows (2023) [en Línea]. [Consultado el 17, septiembre, 2023]. Disponible en Internet: https://dominiogeek.com/comprobar-abrir-cerrar-puertos-windows/

Fortinet. TOP 20 Most Common Types Of Cyber Attacks | Fortinet [en Línea]. (25, septiembre, 2023). [Consultado el 29, septiembre, 2023]. Disponible en Internet: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks/

Infosec Resources. WINDOWS 10 security features | Infosec [en Línea]. (24, septiembre, 2023). [Consultado el 29, septiembre, 2023]. Disponible en Internet: https://resources.infosecinstitute.com/topics/operating-system-security/windows-10-security-features/

IONOS Digital Guide. Protección de sistemas con Intrusion Prevention System e Intrusion Detection System [en Línea]. (8, junio, 2020). [Consultado el 18, septiembre, 2023]. Disponible en Internet: https://www.ionos.es/digitalguide/servidores/seguridad/intrusion-prevention-system-y-detection-system/

KeepCoding Bootcamps. ¿QUÉ ES Metasploit? | KeepCoding Bootcamps. [en Línea]. [Consultado el 10, agosto, 2023]. Disponible en Internet: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad

KeepCoding. Comandos de Meterpreter [en Línea]. (20, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: https://keepcoding.io/blog/comandos-de-meterpreter/

Mandiant. DELETING YOUR Way Into SYSTEM: Why Arbitrary File Deletion Vulnerabilities Matter | Mandiant [en Línea]. (23, septiembre, 2023). [Consultado el 29, septiembre, 2023]. Disponible en Internet: https://www.mandiant.com/resources/blog/arbitrary-file-deletion-vulnerabilities/

Nuclio Digital School. ¿QUÉ ES el Pentesting? Tipos, fases y herramientas [Anónimo]. [en Línea]. [Consultado el 10, agosto, 2023]. Disponible en Internet: https://nuclio.school/que-es-el-pentesting

SECRETARÍA GENERAL DEL SENADO. LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] [en Línea]. [Consultado el 9, agosto, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html .

Secretaria General. LEY 1581 de 2012 Congreso de la República de Colombia [en Línea]. [Consultado el 11, agosto, 2023]. Disponible en Internet: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

SoftZone. ACTIVA O desactiva el Escritorio Remoto de Windows [en Línea]. [Consultado el 17, septiembre, 2023]. Disponible en Internet: https://www.softzone.es/windows/como-se-hace/activar-desactivar-escritorio-remoto-powershell/

SystemExposed. METASPLOIT FRAMEWORK [en Línea]. [Consultado el 10, agosto, 2023]. Disponible en Internet: https://systemexposed.blogspot.com/2014/01/metasploit-framework.html

TheHackerWay. Seguridad en Sistemas y Técnicas de Hacking. [en Línea]. [Consultado el 15, septiembre, 2023]. Disponible en Internet: https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/

ZDNET. THE WINDOWS 10 security guide: How to protect your business [en Línea]. (25, septiembre, 2023). [Consultado el 29, septiembre, 2023]. Disponible en Internet: https://www.zdnet.com/article/the-windows-10-security-guide-how-to-safeguard-your-business/