CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

CARLOS ANDRÉS HERNÁNDEZ OLAYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
BOGOTÁ, 2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

CARLOS ANDRÉS HERNÁNDEZ OLAYA

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

Nombre del tutor
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
BOGOTÁ, 2024

RESUMEN

El desarrollo y aplicación de estrategias de contención para mitigar los riesgos y vulnerabilidades en infraestructuras de Tecnologías de la Información (TI). Tras la ejecución de pruebas de penetración y la implementación de medidas de endurecimiento, se examinan las capacidades técnicas, legales y de gestión necesarias para los equipos Blue Team y Red Team; esto incluye la identificación de vulnerabilidades, la explotación de fallos de seguridad, la remediación de riesgos y la aplicación de medidas de protección. El objetivo principal es encontrar todas las brechas de seguridad ligadas a un proceso de conexión remota reverso, priorizando la mitigación del riesgo y la protección de activos críticos en entornos tecnológicos.

La implementación de esta actividad fortalece la confianza y la estabilidad en el entorno digital dentro de la infraestructura atacada, al tiempo que prepara a la organización para enfrentar las brechas de seguridad, poder adoptar un enfoque integral que combine tecnología, procesos y personas como garante de una defensa efectiva contra las amenazas cibernéticas que día a día se convierten en grandes desafíos.

INDICE

ILUSTRACIONES

CUADROS

GLOSARIO

- Exploit: Código que aprovecha una vulnerabilidad para provocar un comportamiento no deseado en un sistema.

- Payload: Parte de un exploit que realiza una acción específica después de explotar una vulnerabilidad.

- Framework: Conjunto de herramientas y estándares para el desarrollo de software, incluyendo aplicaciones de seguridad.

- Hacking Ético: Evaluación legal de la seguridad de sistemas y redes informáticas.

- Vulnerabilidad: Debilidad en un sistema que podría ser explotada por un atacante.

- Explotación: Aprovechamiento de una vulnerabilidad para obtener acceso no autorizado.

- Intrusión: Acceso no autorizado a un sistema o red informática.

- Malware: Software malicioso diseñado para causar daño o robar información.

- Remediación: Proceso de corrección de vulnerabilidades de seguridad.

- Parcheo: Aplicación de parches de seguridad para corregir vulnerabilidades conocidas.

- Hardening: Fortalecimiento de la seguridad de un sistema mediante configuración y medidas defensivas.

- Meterpreter: Carga útil utilizada en el Metasploit Framework para obtener acceso remoto a sistemas comprometidos.

- Metasploit: Marco de trabajo de seguridad informática para el desarrollo y ejecución de exploits.

INTRODUCCIÓN

Los equipos Blue Team y Red Team desempeñan roles cruciales: el Blue Team se enfoca en fortalecer las defensas y garantizar la seguridad de los sistemas, mientras que el Red Team evalúa la efectividad de estas defensas mediante simulaciones de ataques. En el presente documento se profundizará en las competencias técnicas, legales y de gestión requeridas para ambos equipos, destacando especialmente la importancia de una colaboración efectiva entre ellos para garantizar la resiliencia de la infraestructura digital.

Se analizarán las etapas clave de una prueba de penetración, desde la identificación de vulnerabilidades hasta la implementación de medidas correctivas, con un enfoque en la mejora continua de la postura de seguridad de la organización hackerhouse.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

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

1.2 OBJETIVOS ESPECÍFICOS

- Identificar y documentar las vulnerabilidades existentes en la infraestructura de Tecnologías de la Información (TI), mediante la realización de pruebas de penetración exhaustivas y el análisis detallado de los resultados obtenidos.

- Desarrollar e implementar medidas de remediación y endurecimiento (hardening) específicas, dirigidas a mitigar las vulnerabilidades identificadas y fortalecer la seguridad de la infraestructura TI, en línea con las mejores prácticas y estándares de seguridad.

- Evaluar la efectividad de las estrategias de contención implementadas, comparando los niveles de trabajo reunidos sobre el equipo estratégico PurpleTeam.

2 ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

2.1 PRIMER ENUNCIADO

- Ley 1581 de 2012

La Ley 1581 de 2012, o más reconocida como la Ley de Protección de Datos Personales, es una normativa fundamental que regula el tratamiento y salvaguarda la información personal de los ciudadanos en el país. Esta ley establece los lineamientos, derechos y procedimientos que las organizaciones públicas y privadas deben seguir al reunir, almacenar, utilizar y procesar datos personales.

Entre los aspectos más relevantes abordados por la Ley 1581 de 2012 se encuentra que, en primer lugar, “los fundamentos de protección de datos definen los puntos esenciales que deben guiar el manejo de la información personal, como la finalidad, calidad, seguridad y confidencialidad de los datos”[1]. En segundo lugar, se encuentran los derechos de los titulares de los datos, en donde se reconocen y protegen los derechos del individuo sobre su información personal, como el acceso, rectificación, actualización, inclusión y supresión de datos.

Asimismo, la ley establece las obligaciones de las organizaciones en cuanto al manejo de datos personales, algunas como la implementación de medidas de seguridad adecuadas y la adquisición de la autorización previa y consciente de los poseedores de la información. Finalmente, “la autoridad de control y vigilancia va por parte de la Superintendencia de Industria y Comercio (SIC), supervisa el cumplimiento de la ley y tiene la facultad de imponer sanciones y multas a las organizaciones que incumplan con sus disposiciones”[1].

[1] Data Protected. Protección de Datos. (2023). Disponible en: https://www.dataprotected.com.co/faq-proteccion-datos

En relación con las multas correspondientes, la Ley 1581 de 2012 establece un sistema de sanciones que pueden conllevar multas de hasta 2.000 SMMLMV. La SIC es la entidad encargada de determinar la cuantía de las multas.

- Ley 1273 de 2009

También conocida como la *Ley de Delitos Informáticos* y como se indica en el Diario Oficial sobre la Ley 1273 de 2009[2], aborda principalmente los actos que comprometen la privacidad, integridad y accesibilidad de los datos y sistemas informáticos, así como otras infracciones relacionadas con la manipulación y transferencia no autorizada de activos mediante procesos y entes informáticos

- Artículo 269A: Este artículo establece como delito el acceso no autorizado o no acordado a un sistema informático protegido o no. La pena por este delito es de prisión entre 48 y 96 meses y multa de 100 a 1000 SMLMV.

- Artículo 269B: Se considera delito impedir u obstaculizar el funcionamiento normal de un sistema informático o red de telecomunicaciones sin autorización. La pena es de prisión entre 48 y 96 meses y multa de 100 a 1000 SMMLV. [2]

- Artículo 269C: Este artículo establece como delito la interceptación de datos informáticos sin orden judicial previa. Pena de prisión entre 36 y 72 meses.

- Artículo 269C: Este artículo establece como delito la interceptación de datos informáticos sin orden judicial previa. La pena es de prisión entre 36 y 72 meses.

- Artículo 269D: Se considera delito el daño, destrucción, manipulación o eliminación de información computacional sin permiso. La pena es de prisión entre 48 y 96 meses y multa de 100 a 1000 SMMLV.

[2] Diario Oficial, LEY 1273 DE 2009. (2009). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

- Artículo 269E: Se considera delito la producción, tráfico, distribución o uso de software malicioso sin autorización. La pena es de prisión entre 48 y 96 meses y multa de 100 a 1000 SMMLV.

- Artículo 269F: Este artículo establece como delito obtener, divulgar o modificar datos personales sin autorización. La pena es de prisión entre 48 y 96 meses y multa de 100 a 1000 SMMLV.

- Artículo 269G: Se considera crimen el crear o enviar páginas web con la intención de obtener información personal de manera ilegal. La pena es de prisión entre 48 y 96 meses y multa de 100 a 1000 SMMLV.

- Artículo 269H: Este artículo detalla circunstancias que pueden aumentar las penas por delitos informáticos, como cometer el delito sobre redes estatales, aprovechar la credibilidad otorgada por el titular de los datos, entre otras.

- Artículo 269I: Se considera delito el hurto mediante la manipulación de sistemas informáticos o redes, con las sanciones previstas en el artículo 240 del Código Penal.

- Artículo 269J: Este artículo establece como delito la transferencia no autorizada de activos utilizando manipulación informática, con penas de prisión entre 48 y 120 meses y multa de 200 a 1500 SMMLV.

[2] Diario Oficial, LEY 1273 DE 2009. (2009). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

2.2 SEGUNDO ENUNCIADO

Un CVE constituye un identificador único asignado a una vulnerabilidad específica en la seguridad informática. Este sistema de numeración estandarizado juega un papel fundamental al permitir que cualquier persona se refiera a las mismas vulnerabilidades de forma coherente y precisa. “La estructura de un CVE sigue una convención que consta del formato ‘CVE-year-number’, donde ‘year’ representa el año en que se asigna el identificador, seguido de un número secuencial que denota la vulnerabilidad en ese año. Por ejemplo, CVE-2022-12345”[3].

Por otro lado, Exploit Database se destaca como una plataforma vital que recopila y ofrece exploits de manera pública para diversas vulnerabilidades de software. Los exploits, siendo programas o secuencias de comandos específicamente diseñados, tienen como objetivo aprovechar una vulnerabilidad concreta para obtener acceso no autorizado a sistemas informáticos o ejecutar acciones maliciosas.

La interrelación entre CVE y Exploit Database radica en que los exploits enlistados en Exploit Database suelen hacer referencia a CVE particulares. Los investigadores de seguridad, al descubrir una vulnerabilidad, pueden publicar un exploit que demuestre cómo puede ser explotada dicha vulnerabilidad. “En muchos casos, estos exploits se acompañan del CVE correspondiente en Exploit Database, lo que brinda a los profesionales de la seguridad una comprensión más detallada de la vulnerabilidad y cómo mitigarla. Estos exploits pueden ser utilizados por expertos en seguridad para realizar pruebas de penetración y evaluar la solidez de los sistemas informáticos”[4].

[3] RedHat, El concepto de CVE. (2021). Foro y comunidad, Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

[4] Redacción, KeepCoding. ¿Qué es ExploitDB?. (2022). Tech School, Disponible en: https://keepcoding.io/blog/que-es-exploitdb/

2.3 TERCER ENUNCIADO

El Pentesting, también conocido como test de penetración, es una evaluación de la seguridad informática que busca identificar posibles vulnerabilidades en un sistema y determinar su alcance. Esta práctica, que combina los conceptos de "penetration" y "testing", implica simular un ataque cibernético contra una organización con el fin de poner a prueba y superar sus medidas de seguridad.

Los resultados obtenidos se detallan en un informe que se entrega a la empresa, proporcionándole así la oportunidad de mejorar y reforzar su ciberseguridad. “Esta metodología se considera altamente efectiva para evaluar la eficacia de las defensas de una empresa y fortalecer su postura de seguridad”[5].

- Recopilación y planificación: Se definen los objetivos del Pentesting, se seleccionan los sistemas a evaluar y se determinan los métodos a utilizar. Se recopilan datos necesarios para el test, como escaneos de IP, dominios o puertos, metadatos, etc.

- Análisis de vulnerabilidades: Durante esta etapa se analiza cómo responde el sistema ante una intrusión y se identifican sus vulnerabilidades. Este proceso, combinado con la recopilación y planificación previas.

- Modelado de amenazas: Se explotan las vulnerabilidades para identificar posibles amenazas y determinar las mejoras necesarias en la defensa.

- Explotación del sistema: Se simulan ataques al sistema para evaluar su respuesta y determinar su verdadera vulnerabilidad. En algunos casos, se llevan las defensas del sistema al límite para afinar los resultados.

[5] Nowak, Shirly. ¿Qué es Pentesting?. (2022). nuclio digital school, Disponible en: https://nuclio.school/que-es-el-pentesting/#Que-fases-tiene-el-Pentesting

- Elaboración de informes: Se informa a la empresa sobre los resultados del Pentesting para que pueda implementar mejoras en su seguridad. Se suelen generar dos informes: uno técnico para los administradores del sistema y otro ejecutivo para los directivos de la empresa.

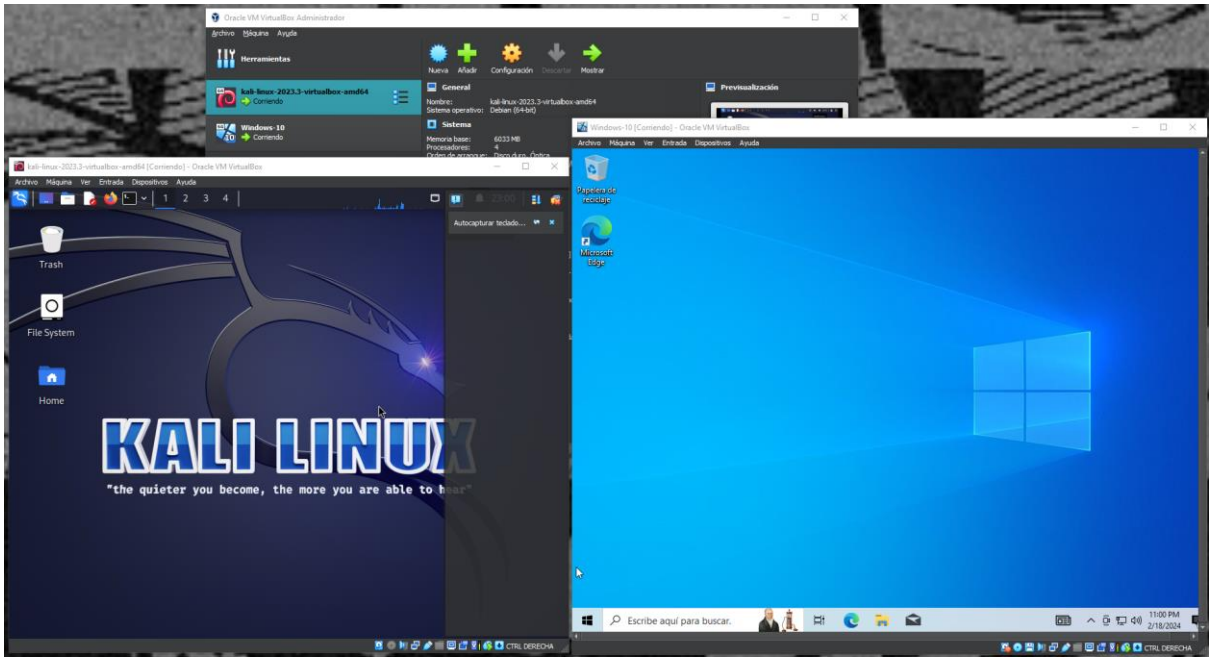
Para la primera etapa de recopilación y planificación en Pentesting, se pueden utilizar varias herramientas tanto de código abierto y algunas comerciales para recopilar información sobre el objetivo del test y definir el alcance del Pentesting. Algunas de estas herramientas son:

- Maltego: Una herramienta de inteligencia de código abierto que facilita la recopilación y análisis de datos relacionados con individuos, organizaciones y sus interconexiones.
- Nmap: Es una herramienta para el scann de puertos, es de código abierto que permite descubrir dispositivos y servicios en una red, identificando así posibles puntos de entrada.
- Shodan: Un motor de búsqueda enfocado en dispositivos conectados a la red, que posibilita la detección de sistemas en situación vulnerable o con configuraciones deficientes.
- Metasploit: Aunque es conocido principalmente por su función como framework de explotación, también puede ser utilizado en la fase de recopilación de información para identificar posibles vulnerabilidades.

Aquí se definen los objetivos del test, se identifican los sistemas a evaluar y se determinan los métodos a utilizar. Sin una adecuada planificación, el Pentesting puede carecer de dirección y no alcanzar sus objetivos de manera efectiva. Además, esta etapa proporciona una comprensión inicial del entorno objetivo, lo que permite al equipo de Pentesting identificar posibles vulnerabilidades y desarrollar estrategias adecuadas para su evaluación y explotación en etapas posteriores.

2.4 CUARTO ENUNCIADO

Ilustración 1. Evidencia banco de trabajo



Fuente propia

3 ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL

A partir de la información del diario Oficial[6], los enumerados 1 y 2 son análisis basados a partir del apoyo de la redacción de la Ley 1273 de 2009.

3.1 PRIMER ENUNCIADO

- Cláusula 2: Establece que la parte receptora se compromete a no divulgar la información confidencial ni los procesos ilegales dentro de HackerHouse, lo cual es ilegal si el acuerdo implica encubrir actividades ilícitas o delitos.

- Cláusula 5: Allí se mencionan ciertos términos como "datos de chuzadas", "interceptación ilegal de información" y "accesos abusivos a sistemas informáticos" como información confidencial, por lo que estos términos podrían sugerir actividades ilegales o cuestionables.

- Cláusula 4: Enumera las obligaciones de la parte receptora, incluyendo la responsabilidad de no denunciar actividades sospechosas de espionaje o cualquier otro proceso relacionado con la apropiación de información de terceros, lo cual podría ser considerado ilegal si impide que la parte receptora informe de actividades delictivas a las autoridades competentes.

- Cláusula 6: Analizar las actividades realizadas por los equipos Red Team y Blue Team de una empresa dentro de los parámetros éticos y legales establecidos. Esto podría ser ilegal si implica encubrir actividades delictivas o inhibir la acción legal adecuada.

[6] Diario Oficial, LEY 1273 DE 2009. (2009). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

3.2 SEGUNDO ENUNCIADO

- Cláusula 1: Esta cláusula podría considerarse ilegal si implica encubrir actividades ilícitas o delitos. En este caso, podría estar violando el artículo 269F de la Ley 1273 de 2009, que tipifica como delito la violación de datos personales.

  Esta ley establece sanciones para aquellos que, sin estar facultados para ello, obtengan, divulguen o utilicen datos personales de forma ilegal.

- Cláusula 3: Los términos mencionados como "datos de chuzadas", "interceptación ilegal de información" y "accesos abusivos a sistemas informáticos" podrían sugerir actividades ilegales o cuestionables, lo cual podría ser contrario a la ley. En este caso, se podría estar violando el artículo 269D de la Ley 1273 de 2009, que establece sanciones para aquellos que destruyan, dañen, alteren o supriman datos informáticos sin autorización.

- Cláusula 4: La obligación de no denunciar actividades sospechosas de espionaje o cualquier otro proceso relacionado con la apropiación de información de terceros podría ser considerada ilegal si impide que la parte receptora informe de actividades delictivas a las autoridades. Esto podría violar el artículo 269G de la Ley 1273 de 2009, que establece sanciones para aquellos que suplanten sitios web para capturar datos personales.

- Cláusula 6: Esta cláusula podría ser ilegal si implica encubrir actividades delictivas o inhibir la acción legal adecuada. La acción en cuestión podría implicar una contravención al artículo 269C de la Ley 1273 de 2009, el cual prescribe penalidades para aquellos que accedan a datos informáticos sin una orden judicial previa.

3.3 TERCER ENUNCIADO

Basándome en el Código de Ética del COPNIA[7], veo varias disposiciones y prohibiciones que consideraría al evaluar la aceptación de un trabajo o contrato, especialmente aquellos relacionados con actividades ilegales propuestas por las cláusulas analizadas anteriormente. Como profesional, es mi responsabilidad cumplir con los requisitos del COPNIA y evitar cualquier actividad propia ilegal.

Siento que tengo un deber especial con la sociedad. Debo utilizar mis conocimientos para contribuir al bien público y al progreso social, por lo tanto, no puedo aceptar trabajos que vayan en contra de las leyes vigentes o que estén fuera de mi ámbito de competencia profesional, como las actividades ilegales propuestas por las cláusulas del contrato de la empresa de hacking y asuntos informáticos.

Respecto a mis colegas y otros profesionales, entiendo la importancia de actuar con prudencia y diligencia al emitir juicios sobre sus acciones. Debo evitar cualquier práctica de competencia desleal y siempre respetar la propiedad intelectual de mis colegas.

Con esto, puedo decir que cualquier contrato que me obligue a encubrir actividades ilegales o que plantee términos que sugieran actividades cuestionables, como los mencionados en las cláusulas del contrato de la empresa HackerHouse, estaría en conflicto con estos principios éticos y legales; y en relación con las inhabilidades e incompatibilidades, comprendo que debo evitar cualquier conflicto de interés al actuar como asesor de múltiples empresas involucradas en actividades afines sin obtener el consentimiento expreso de todas las partes involucradas podría generar conflictos de interés y violar los principios éticos y legales establecidos.

[7] COPNIA. Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (2022). Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

3.4 CUARTO ENUNCIADO

El reciente ciberataque sufrido por Keralty, resalta todo el proceso actual de ciberataques que están sucediendo de manera mediática hacia los sistemas privados y públicos indiscriminadamente. La revelación de que los atacantes han obtenido 0,7 terabytes de información institucional, incluidos estados financieros y datos personales, plantea serias preocupaciones sobre la seguridad cibernética y la protección de la información en Colombia.

En este contexto, es crucial mencionar las leyes colombianas pertinentes que abordan la ciberdelincuencia y protegen la información personal. La Ley 1273 de 2009[8], que establece disposiciones sobre delitos informáticos y sanciones relacionadas, es fundamental para combatir actividades como el ciberataque sufrido por el Grupo Keralty. La normativa vigente, denominada Ley 1581 de 2012 o Ley de Protección de Datos Personales, proporciona directrices y protocolos para el manejo y control de intervención cuando se habla de la información de la población. Esta ley es relevante en el contexto del ciberataque, ya que protege los datos personales comprometidos por los piratas informáticos y establece obligaciones para las empresas en términos de seguridad.

Finalmente, la Ley 1755 de 2015, que aborda la protección de la infraestructura crítica de información, también puede ser relevante en el contexto del ciberataque al Grupo Keralty. Esta ley establece parámetros que se dedican a la protección de sistemas que pueden contar como infraestructura crítica, para el funcionamiento del país y puede ser aplicable en casos donde la infraestructura de salud se vea comprometida por actividades delictivas en línea.

[8] Portafolio, Ataque informático a Sanitas no comprometió información de usuarios. (2022). Disponible en: https://www.portafolio.co/negocios/empresas/eps-sanitas-detalles-del-ciberataque-que-sufrio-grupo-keralty-575968

4 ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

4.1 PRIMER ENUNCIADO

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

- Meterpreter: Es un potente y versátil payload de Metasploit, diseñado para proporcionar un control total sobre los sistemas comprometidos durante una evaluación de penetración o un ataque informático. “Permite al atacante realizar una amplia gama de actividades, como la ejecución de comandos en el sistema comprometido, la extracción de información confidencial, la manipulación de archivos y la elevación de privilegios”[10]. Meterpreter está diseñado para evadir la detección de antivirus y otras medidas de seguridad, lo que lo convierte en una herramienta popular.

- Metasploit: Es un marco de pruebas de penetración de código abierto ampliamente utilizado por profesionales de la seguridad informática y hackers éticos para llevar a cabo evaluaciones de seguridad en sistemas informáticos. Esta tiene una cantidad considerable de herramientas y acciones para descubrir, explotar y mitigar vulnerabilidades en redes, sistemas operativos y aplicaciones.

  Metasploit proporciona una interfaz unificada para realizar pruebas de penetración, desde la fase de descubrimiento de vulnerabilidades hasta la explotación y el mantenimiento del acceso. Su gran comunidad de usuarios contribuye constantemente con nuevos módulos y exploits, lo que lo convierte en una herramienta dinámica y en constante evolución.

[10] Adastra. Conceptos Basicos de Meterpreter – MetaSploit Framework. (2022). thehackerway. Disponible en: https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/

- Consola msfvenom: Es una herramienta incluida en el marco Metasploit que se utiliza para la generación y codificación de payloads, también conocidos como shellcodes o códigos de shell. Permite a los usuarios crear payloads personalizados que pueden ser utilizados para explotar vulnerabilidades en sistemas informáticos durante pruebas de penetración.

  Msfvenom ofrece una amplia gama de opciones y parámetros para personalizar los payloads según las necesidades específicas de la situación, como la plataforma del objetivo, la arquitectura del sistema y el tipo de conexión. Puede generar payloads en una variedad de formatos, incluyendo binario, script, shellcode y código fuente, por lo que la hace una herramienta versátil para los profesionales del tema.

- Kali Linux: Es una distribución de Linux basada en Debian diseñada específicamente para pruebas de penetración, evaluaciones de seguridad y auditorías forenses.

  Es una herramienta integral para profesionales de la seguridad informática y hackers éticos, ya que proporciona un gran repertorio de herramientas preinstaladas para ejecutar diversas tareas relacionadas con la seguridad, algunas de estas y bien conocidas como el escaneo de vulnerabilidades, análisis de redes, auditorías de seguridad web, recuperación de datos y análisis forense de sistemas.

  Kali Linux se desarrolla y mantiene por Offensive Security y se distribuye de forma gratuita, es por esto por lo que se usa usualmente por la comunidad de seguridad informática. Su enfoque en la seguridad y la privacidad, junto con su capacidad de personalización y su amplia documentación, la convierten en una de las primeras opciones a usar en la materia.

4.2 SEGUNDO ENUNCIADO

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

- Sistema operativo y arquitectura: La máquina objetivo se describe como un sistema Windows 10 a 64 bits. Esta información fue importante para comprender las vulnerabilidades y exploits que afectan este tipo de sistemas.

- Estado de los sistemas de seguridad: Se menciona que tanto los sistemas de seguridad del sistema operativo (Firewall, Windows Defender) como los externos (antivirus) estaban totalmente desactivados, lo cual sugiere una vulnerabilidad significativa en la infraestructura de seguridad de la máquina y la hace más susceptible a ataques.

- Archivo de texto en el escritorio: El administrador de la computadora afectada informa sobre la presencia de un archivo de texto en el escritorio con un formato específico: "CarlosHernandez_1032442766_17032024". Sin embargo, este archivo ya no se encontraba en la ubicación indicada. Este detalle indica la posible actividad maliciosa relacionada con la manipulación o eliminación de archivos por parte del atacante.

- Ejecución de un archivo .exe: Se menciona que el administrador ejecutó un archivo .exe llamado "PoC_1032442766" en la computadora afectada. Este archivo, enviado a través de WhatsApp Web por un compañero de trabajo, podría haber sido la entrada para el ataque ya que debemos tener en cuenta que la ejecución de archivos desconocidos representa un riesgo de seguridad significativo y puede permitir la introducción de malware en el sistema.

4.3 TERCER ENUNCIADO

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

Para identificar los fallos de seguridad en la máquina Windows 10, se utilizó la herramienta Metasploit, específicamente a través del uso de MSFVenom y Meterpreter. MSFVenom se empleó para crear un payload malicioso en forma de un archivo ejecutable (.exe), mientras que Meterpreter se utilizó para obtener acceso remoto al sistema comprometido una vez que el archivo fue ejecutado.

En cuanto al puerto utilizado por la aplicación específica mencionada en el anexo, se indica que el puerto 443 fue empleado para la escucha de la conexión entrante que establece el Meterpreter una vez que se ejecuta el archivo .exe malicioso en la máquina Windows 10 comprometida. Este puerto suele estar abierto y es comúnmente utilizado para comunicaciones seguras a través del protocolo HTTPS.

4.4 CUARTO ENUNCIADO

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

El ataque a la máquina Windows 10 X64 se lleva a cabo mediante la ejecución de un archivo malicioso .exe, creado utilizando MSFVenom, que contiene un payload diseñado para explotar una vulnerabilidad en el sistema operativo objetivo. Una vez que el usuario ejecuta este archivo malicioso, se establece una conexión reversa con la máquina atacante a través del puerto 443. Esta conexión permite al atacante obtener un control remoto completo sobre la máquina comprometida. El atacante puede realizar una variedad de acciones maliciosas, como acceder y robar datos sensibles, instalar software adicional para espiar al usuario o utilizar la máquina comprometida como parte de una botnet para lanzar ataques adicionales.

El siguiente gráfico ilustra el siguiente flujo del ataque:

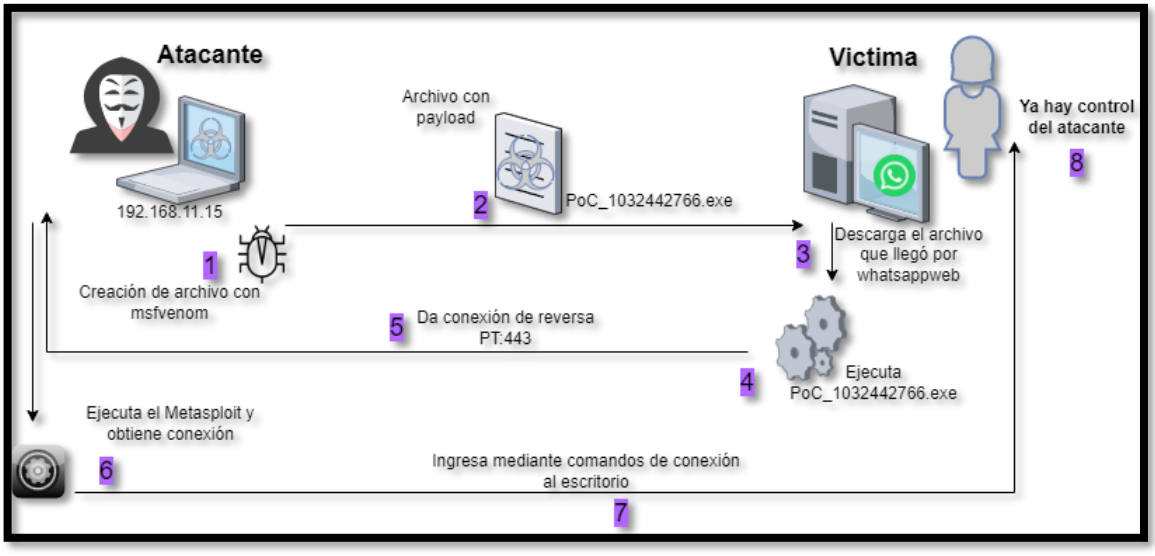
- Creación del payload malicioso: Se utiliza MSFVenom para crear un archivo .exe malicioso que contiene el payload diseñado para explotar la vulnerabilidad en la máquina Windows 10.

- Ejecución del archivo malicioso: El usuario descarga y ejecuta el archivo malicioso en la máquina Windows 10 comprometida.

- Conexión reversa al atacante: Una vez que se ejecuta el archivo malicioso, se establece una conexión reversa desde la máquina comprometida al atacante a través del puerto 443.

- Control remoto de la máquina comprometida: El atacante obtiene acceso remoto completo a la máquina comprometida. Puede realizar diversas acciones maliciosas, como robar datos, instalar software adicional o utilizar la máquina para lanzar más ataques.

Ilustración 2. Flujo del ataque



Fuente propia

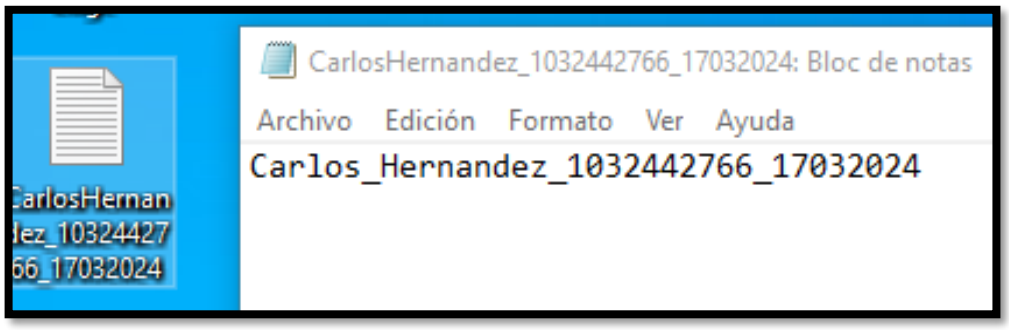
1. Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

Paso 1: Maquinas dispuestas para POC y archivo.

Ilustración 3. Máquinas y redes

Fuente propia

Ilustración 4. Archivo txt



Fuente propia

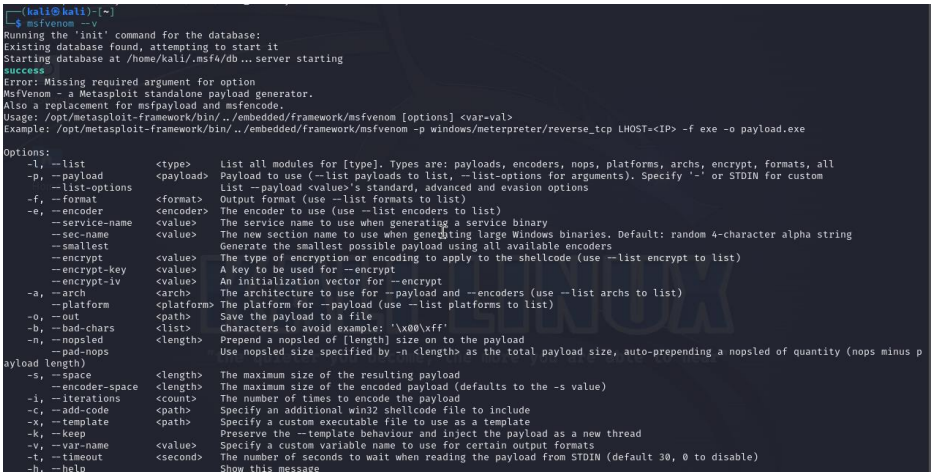
Paso 2: Desactivación de controles

Ilustración 5. FW, AV y otros desactivados

Fuente propia

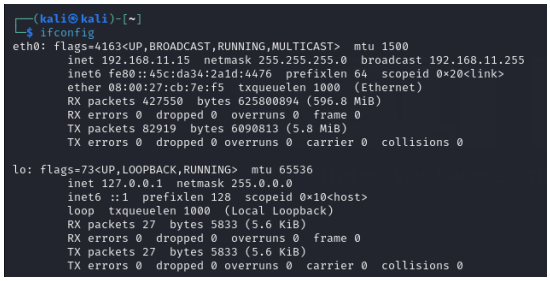
Paso 3. Msfvenom y red

Ilustración 6. Comprobación del recurso



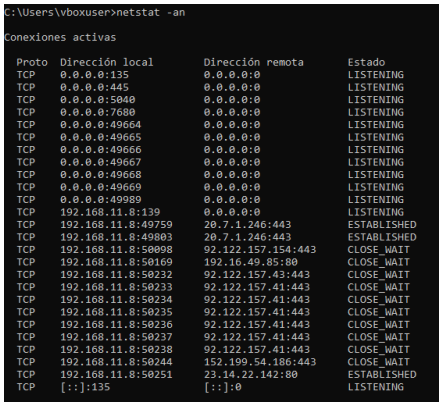
Fuente propia

Ilustración 7. IP máquina atacante



Fuente propia

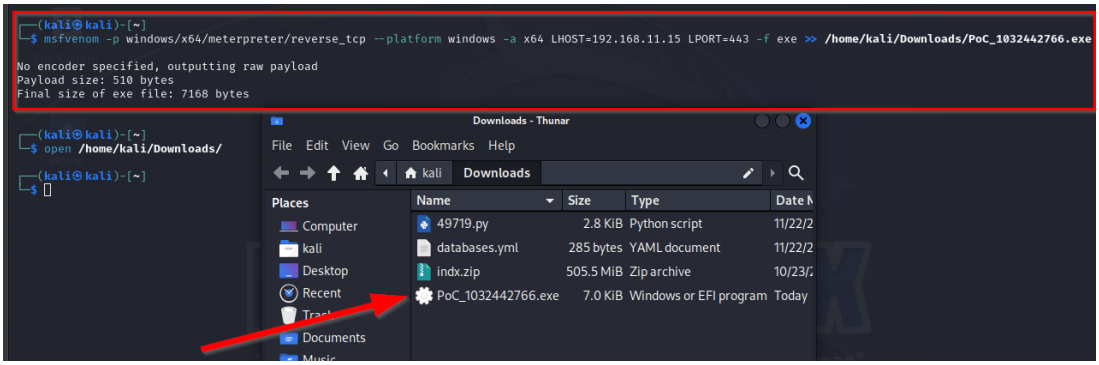
Ilustración 8. Estado de los puertos maquina atacada



Fuente propia

Paso 4. Creación de la carga útil

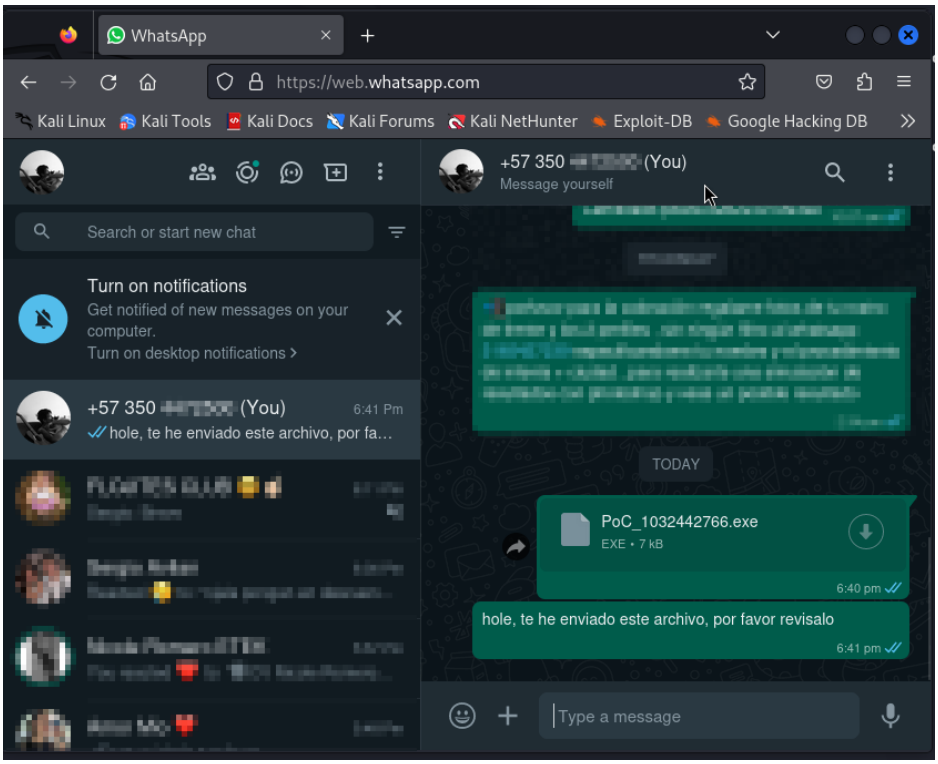
Ilustración 9. Carga útil



Fuente propia

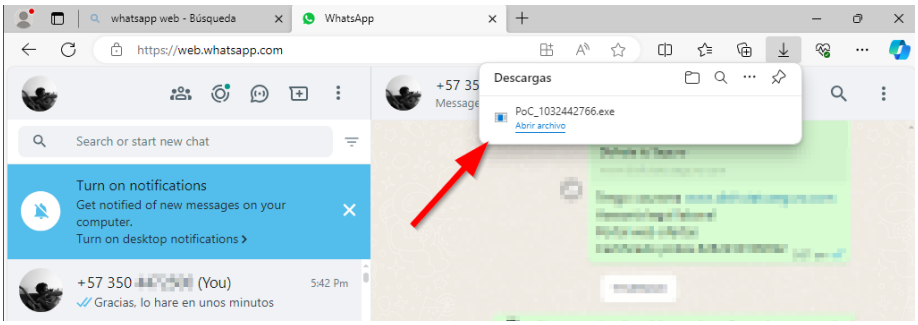
Paso 5. Emisión de archivo

Ilustración 10. Archivo mediante Whatsapp



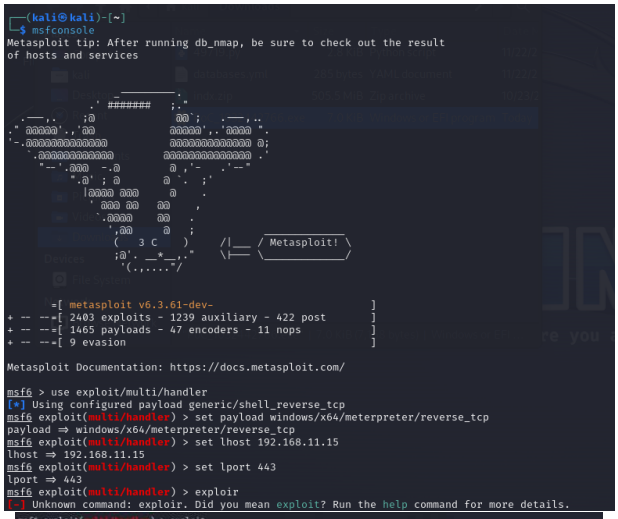
Fuente propia

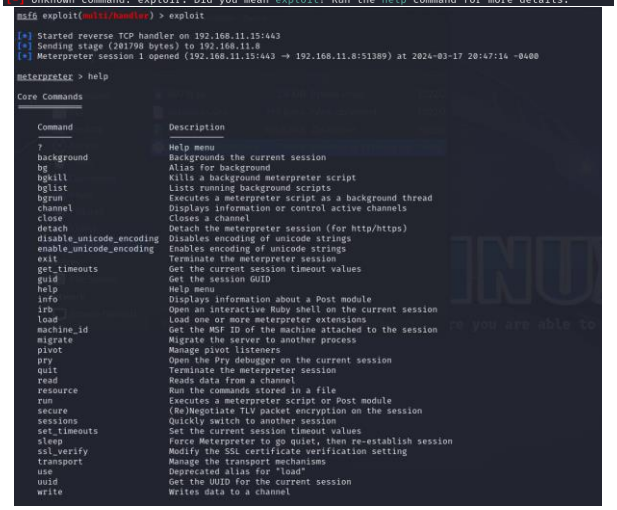
Ilustración 11. Descarga del archivo en Windows



Fuente propia

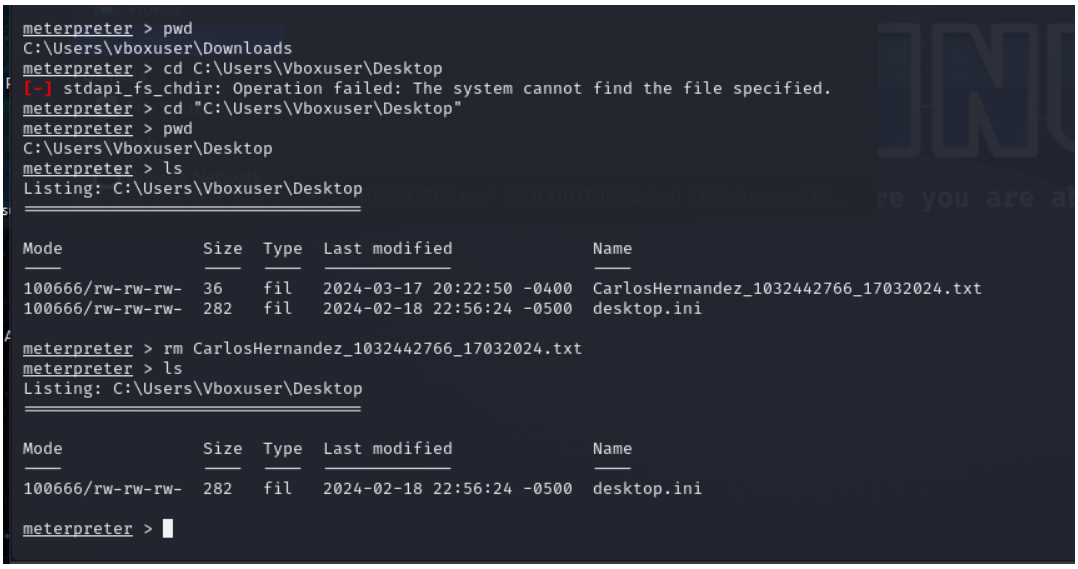
Ilustración 12. Carga el exploit y comandos básicos





Fuente propia

Ilustración 13. Ejecución de exploit



Fuente propia

Ilustración 14. Evidencia de eliminación

Fuente propia

5 ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1 PRIMER ENUNCIADO

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

Es crucial contar con un **Plan de Respuesta a Incidentes de Ciberseguridad** que proporcione un marco de trabajo organizado para abordar posibles ciberataques. Este plan debe ser difundido y probado regularmente en toda la organización para garantizar su efectividad.

Para desarrollar este plan, se pueden tomar como referencia estándares ampliamente reconocidos a nivel internacional, como el “Computer Security Incident Handling Guide del NIST y la norma ISO/IEC 27035:2016 de Gestión de Incidentes de Seguridad de la Información”[13]. El *Plan de Respuesta a Incidentes* consta típicamente de cuatro fases principales:

Planificación y preparación: Durante esta etapa, se definen roles y responsabilidades, se evalúan los riesgos y se establecen herramientas y procesos para la prevención y detección de ciberataques. También se conforma un Equipo de Respuesta a Incidentes y se establecen mecanismos de comunicación.

Detección y análisis: En esta fase, se monitorean los sistemas en busca de posibles indicadores de compromiso y se investigan los eventos sospechosos para determinar su naturaleza y alcance. Se utilizan herramientas de seguridad y se analizan registros de eventos para identificar cualquier actividad inusual o maliciosa.

[13] Parra, Francis. ¿Qué hacer en caso de un ciberataque? (2020). Netdata. Disponible en: https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

Respuesta (Contención, erradicación y recuperación): Una vez que se detecta un incidente, se toman medidas para detener su propagación, eliminar cualquier amenaza existente y restaurar los sistemas afectados a un estado operativo normal. Esto implica acciones de contención, erradicación y recuperación.

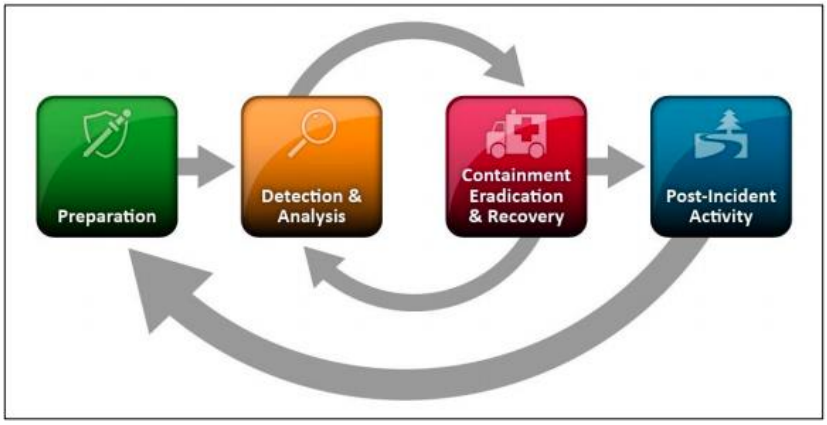
Cuadro 1. Ejemplos de estrategias de contención

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del root	Apagado del sistema
Reconocimiento	Scanning de puertos	Incorporación de reglas de filtrado en el firewall

Fuente: MINTIC

Acciones Post-Incidente: Finalmente, se documentan las lecciones aprendidas y se identifican mejoras para fortalecer la capacidad de respuesta ante futuros incidentes. Se recopilan datos sobre la gestión del incidente, las acciones tomadas y las áreas de mejora, y se utilizan para actualizar y mejorar el plan de respuesta a incidentes.

Ilustración 15. Incident Response Life Cycle



Fuente: NIST https://acortar.link/ozrXpb

5.2 SEGUNDO ENUNCIADO

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

Desconexión de la red:

- Se procedió a desconectar físicamente el cable de red del sistema comprometido para evitar cualquier comunicación no autorizada.
- Se desactivaron las conexiones inalámbricas, como Wi-Fi y Bluetooth, para prevenir posibles accesos remotos no deseados.

Identificación y eliminación del archivo malicioso:

- Se utilizó y activo los controles de seguridad de Windows, como el firewall y los controles de tiempo real.
- Se llevaron a cabo análisis exhaustivos de procesos en ejecución y servicios activos para detectar posibles comportamientos anómalos.
- Se emplearon herramientas de análisis de comportamiento conocidas como Sysinternals Suite, para identificar y mitigar actividades maliciosas en tiempo real, donde se encontró el archivo malicioso.

Restauración desde una copia de seguridad conocida:

- Se optó por restaurar el sistema desde una copia de seguridad previamente verificada, asegurándose de regresar a un estado conocido y limpio.

Actualización del sistema operativo y software:

- Se verificaron y aplicaron todas las actualizaciones pendientes del sistema operativo y del software instalado desde los sitios oficiales de Windows.

- Se configuró el sistema para actualizar automáticamente en el futuro, garantizando la mitigación de vulnerabilidades conocidas.

2.5 Revisión y fortalecimiento de la configuración de seguridad:

- Se revisaron y aplicaron las directivas de seguridad locales y de dominio mediante herramientas de directivas de grupo para deshabilitar servicios y características innecesarias.
- Se configuró el firewall de Windows para bloquear tráfico no autorizado y limitar conexiones entrantes y salientes según las necesidades del entorno.

2.6 Análisis forense del sistema:

- Se llevaron a cabo análisis forenses utilizando herramientas como Volatility Framework y Autopsy para recopilar y examinar artefactos del sistema.
- Se investigaron registros de eventos de Windows y el sistema de archivos en busca de indicios de actividad maliciosa o cambios no autorizados.

2.7 Implementación de medidas de detección y prevención:

- Se contemplan controles adicionales como sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear y bloquear actividades maliciosas.

El paso a paso que se ha contemplado, está basado sobre el proceso del gobierno de Australia como base fundamental para la hardenización[14].

[14] Australian, Government. Hardening Microsoft Windows 10 version 21H1 Workstations. (2021). v2, pg [6-49]. Disponible en: https://www.cyber.gov.au

5.3 TERCER ENUNCIADO

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

Cuadro 2. Comparativas de equipos

Equipos Comparativas	Blue Team	Red Team	Purple Team	CSIRT
Función	El equipo Blue Team se enfoca en la defensa y protección de los sistemas de información de una organización.	El equipo Red Team actúa como un adversario simulado, realizando pruebas de penetración y evaluaciones de seguridad para identificar debilidades en los sistemas y procesos de una organización.	El equipo Purple Team actúa como un puente entre el Blue Team y el Red Team, facilitando la colaboración y el intercambio de conocimientos entre ambos.	Los equipos de respuesta a incidentes informáticos son responsables de gestionar y responder a incidentes de seguridad cibernética dentro de una organización.
Actividades	Monitorean la red, detectan amenazas, implementan controles de seguridad, responden a incidentes y llevan a cabo operaciones de seguridad defensiva.	Ejecutan ataques controlados, utilizan técnicas de hacking ético para encontrar vulnerabilidades y evalúan la efectividad de las defensas de seguridad.	Coordina ejercicios de simulación de ataques donde el Red Team realiza pruebas de penetración simuladas y el Blue Team responde y mejora sus defensas en tiempo real. También ayuda a interpretar los resultados y a implementar mejoras en las defensas de seguridad.	Detectan, investigan, contienen y remedian incidentes de seguridad, coordinan la respuesta a incidentes y realizan análisis forenses para determinar el alcance y el impacto de los incidentes.
Objetivo	Proteger activos, datos y sistemas contra ataques cibernéticos.	Mejorar la postura de seguridad de una organización al identificar y remediar vulnerabilidades antes de que sean explotadas por amenazas reales.	Fomentar una cultura de seguridad colaborativa y mejorar la preparación y capacidad de respuesta frente a amenazas cibernéticas.	Minimizar el tiempo de inactividad, mitigar el daño y restaurar la normalidad operativa después de un incidente de seguridad. También trabajan en la mejora continua de los procesos de respuesta a incidentes y en la prevención de futuros incidentes.

Fuente UNIR

5.4 CUARTO ENUNCIADO

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

Trabajar con CIS es esencial para equipos Blue Team en seguridad cibernética, ya que ofrece estándares reconocidos globalmente que reducen riesgos al mitigar vulnerabilidades y prevenir ataques. “Las actualizaciones regulares y la comunidad global de CIS facilitan la mejora continua y el intercambio de conocimientos, fortaleciendo así la seguridad de manera efectiva”[16].

- Función de CIS en equipos Blue Team:

- *Guías de seguridad:* CIS ofrece una amplia gama de guías de seguridad detalladas, conocidas como CIS Benchmarks, que proporcionan recomendaciones específicas para asegurar sistemas operativos, aplicaciones y dispositivos de red.

- *Configuraciones seguras:* Estas guías describen configuraciones seguras recomendadas para una variedad de tecnologías, incluidos sistemas operativos, aplicaciones y dispositivos.

- *Mejores prácticas:* Las pautas de CIS se fundamentan en las prácticas óptimas de la industria y en las sugerencias de especialistas en seguridad informática.Estas prácticas pueden ayudar a prevenir vulnerabilidades comunes y mitigar riesgos.

- *Evaluación de cumplimiento:* Los equipos Blue Team pueden utilizar las guías de CIS como referencia para evaluar y mejorar el cumplimiento de seguridad de sus sistemas. Esto implica comparar la configuración actual de los sistemas con las recomendaciones de CIS y realizar ajustes según sea necesario.

[16] Manage Engine. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)? (2023). Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

- Tutorial para encontrar recursos de CIS

1. Sitio web de CIS: Visita el sitio web oficial de CIS en https://www.cisecurity.org/.

Ilustración 16. Cabecera de guía virtual

Fuente CIS Security

2. Explorar recursos: Navega por el sitio para acceder a los recursos disponibles. Esto incluye las guías de CIS Benchmarks, herramientas de evaluación de cumplimiento, informes de investigaciones de seguridad y más.

3. CIS Benchmarks: Encuentra las guías de CIS Benchmarks específicas para las tecnologías que te interesan. Puedes buscar por sistema operativo, aplicación o dispositivo de red.

4. Descargar guías: Descarga las guías de CIS Benchmarks relevantes en formato PDF o accede a ellas en línea para revisar las recomendaciones detalladas.

5. Implementación práctica: Utiliza las guías de CIS Benchmarks como referencia para implementar configuraciones seguras en tus sistemas y mejorar la postura de seguridad de tu organización.

5.5 QUINTO ENUNCIADO

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

Cuadro 3. Diferencias entre SIEM y XDR

Controles Puntos a comparar	SIEM	XDR
Alcance y funcionalidad	Se enfoca en la recopilación, correlación y análisis de datos de seguridad de una amplia gama de fuentes, como registros de eventos, tráfico de red y datos de sistemas.	Amplía el alcance de SIEM al agregar capacidades de detección y respuesta extendidas que abarcan múltiples capas de seguridad, incluyendo endpoints, redes y cargas de trabajo en la nube.
Fuentes de datos	Integra datos de una variedad de fuentes, como registros de eventos, firewalls, sistemas de detección de intrusiones (IDS/IPS), y sistemas de prevención de pérdida de datos (DLP).	También integra datos de múltiples fuentes, pero se centra más en los datos generados por endpoints, como sistemas finales, servidores y dispositivos IoT.
Análisis y correlación	Utiliza análisis de eventos en tiempo real y correlación de datos para identificar patrones y anomalías que podrían indicar actividades maliciosas.	Emplea análisis avanzados, como inteligencia artificial y aprendizaje automático, para detectar amenazas sofisticadas y realizar correlaciones entre eventos de seguridad en múltiples vectores.
Respuesta a incidentes	Proporciona capacidades básicas de respuesta a incidentes, como alertas y notificaciones, pero la respuesta puede requerir intervención manual.	Ofrece capacidades de respuesta automatizada y orquestación de seguridad para contener rápidamente las amenazas detectadas y reducir el tiempo de exposición.
Enfoque vs. solución	Suele ser una plataforma integral que puede requerir una configuración y personalización significativas para adaptarse a las necesidades específicas de seguridad de una organización.	A menudo se presenta como una solución integrada y lista para usar que combina detección avanzada, análisis y respuesta en una única oferta.

Fuente Arnal, Carlos de WatchGuard

5.6 SEXTO ENUNCIADO

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

“La Licencia Pública General (GPL) es un tipo de licencia de código abierto que garantiza a los usuarios la libertad de usar, estudiar, modificar y distribuir el software”[18].

Requiere que el código fuente esté disponible para cualquier persona que reciba el software, y cualquier modificación debe distribuirse bajo los mismos términos. La GPL fomenta la colaboración y la innovación al permitir que la comunidad contribuya al desarrollo del software.

- Snort:

“Es un sistema de detección y prevención de intrusiones de red (NIDS/NIPS) de código abierto y ampliamente utilizado. Utiliza reglas de firma para detectar patrones de tráfico malicioso en tiempo real”[18].

Características:

- Capacidad de análisis de paquetes en tiempo real.
- Motor de reglas flexible que permite personalizar las políticas de detección.
- Compatible con una amplia gama de protocolos de red.
- Sitio web: https://www.snort.org/

[18] Cody, Wilson. Evaluating the Efficacy of Network Forensic Tools: A Comparative Analysis of Snort, Suricata, and Zeek in Addressing Cyber Vulnerabilities. (2024). SANS. Disponible en: https://www.sans.org

- Suricata:

Es otro NIDS/NIPS OSSINT - sin costo, robusto y versátil. Utiliza un motor de reglas basado en lenguaje YAML para detectar y prevenir intrusiones en redes.
Características:

- Soporte para reglas de Snort y reglas de Suricata propias.
- Inspección de tráfico en tiempo real con capacidad para realizar análisis de paquetes a alta velocidad.
- Integración con otros sistemas de seguridad y herramientas de análisis de seguridad.
- Sitio web: https://suricata.io/

- Bro (ahora Zeek):

Ahora conocido como Zeek, es una poderosa plataforma de monitorización de red de código abierto que se centra en el análisis de tráfico de red y la generación de registros detallados para la detección de amenazas.

Características:

- Análisis profundo del tráfico de red para identificar actividades maliciosas.
- Generación de registros detallados en tiempo real sobre conexiones de red, protocolos y actividades sospechosas.
- Extensible mediante scripts y plugins para personalizar y ampliar su funcionalidad.
- Sitio web: https://zeek.org/

6 ETAPA 5: SOCIALIZACIÓN DE INFORME TÉCNICO

6.1 PRIMER ENUNCIADO

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

La integración de equipos Blue Team, Red Team y Purple Team en el campo de la ciberseguridad es una acción fundamentel para fortalecer las defensas y la capacidad de respuesta de una organización frente a las crecientes amenazas cibernéticas. “El equipo Blue Team se enfoca en la defensa activa de la infraestructura de TI, implementando y manteniendo medidas de seguridad, monitoreando la red en busca de anomalías y respondiendo a incidentes de seguridad. Por otro lado, el equipo Red Team lleva a cabo pruebas de penetración autorizadas y simulaciones de ataques para identificar debilidades en las defensas existentes” 19. Su objetivo es actuar como un adversario real para poner a prueba la resiliencia de la organización frente a amenazas externas e internas.

El equipo Purple Team desempeña un papel crucial como facilitador entre el Blue Team y el Red Team. Coordina la colaboración entre ambos equipos, compartiendo información sobre las tácticas y técnicas utilizadas por el Red Team y ayudando al Blue Team a mejorar sus defensas en función de los hallazgos. Es importante tener en cuenta el Purple Team promueve un enfoque proactivo hacia la seguridad cibernética, identificando áreas de mejora y brindando recomendaciones para fortalecer la postura de seguridad de la organización.

En conjunto, la colaboración y la integración de estos equipos permiten una evaluación más completa de la postura de seguridad de la organización y facilitan la implementación de medidas correctivas efectivas. Esta sinergia promueve una cultura de seguridad cibernética sólida y adaptable.

6.2 SEGUNDO ENUNCIADO

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

A continuación, se presentan algunas políticas y recomendaciones clave que, si bien son básicas y elementales, no pueden faltar en ninguna organización, y deben ser adaptables a la necesidad y propuesta del negocio. Es clave recordar que los parámetros expuestos son de implementación sugerida según el control y herramienta tecnológica que se maneje.

1. Garcia, Jorge[19], expone algunas políticas de acceso y control de usuarios:

- Desplegar un sistema de administración de identidades y accesos (IAM) para supervisar y regular el acceso a los activos de tecnología de la información.
- Implementar la estrategia de privilegios mínimos, otorgando a cada usuario únicamente los permisos esenciales.
- Instaurar políticas de autenticación sólidas, como la utilización de contraseñas robustas, autenticación de dos factores (2FA) y políticas de cambio regular de contraseñas.

2. Política de seguridad de la red:

- Configurar firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS) para salvaguardar la red frente a ataques.
- Establecer la segmentación de red para restringir la propagación de amenazas y minimizar las consecuencias de posibles brechas de seguridad.
- Utilizar tecnologías de cifrado, como VPNs y SSL/TLS, para proteger la comunicación entre dispositivos y redes.

[19] García, Jorge. Políticas de seguridad: Por qué son importantes para tu negocio. (2024). deltaprotect. Disponible en: https://www.deltaprotect.com/blog/politicas-de-seguridad

3. Política de gestión de vulnerabilidades:

- Realizar evaluaciones periódicas de vulnerabilidades y parchear sistemas y aplicaciones de manera regular para mitigar posibles riesgos de seguridad.
- Desarrollar un procedimiento de administración de parches que contemple la evaluación del impacto, pruebas de compatibilidad y una implementación segura de las actualizaciones.
- Implementar medidas de mitigación para riesgos de seguridad conocidos mientras se espera la aplicación de parches.

4. Política de concientización y capacitación:

- Instruir al personal en el correcto manejo de tecnología, abordando la identificación de riesgos, la gestión adecuada de contraseñas y la identificación de correos electrónicos fraudulentos.
- Implementar programas periódicos de sensibilización en seguridad para mantener al personal al tanto de las últimas amenazas y estrategias de seguridad óptimas.

5. Política de respuesta ante incidentes:

- Desarrollar un protocolo de acción frente a eventos inesperados que englobe directrices definidas para identificar, reportar, investigar y restaurar incidentes de seguridad.
- Asignar un grupo especializado en responder a incidentes y ofrecer entrenamiento periódico para asegurar una reacción pronta y eficiente ante posibles contratiempos de seguridad.

6.3 TERCER ENUNCIADO

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

A lo largo de las etapas, se han explorado diversos escenarios y aspectos relacionados con la ciberseguridad, proporcionando un panorama completo de los desafíos y oportunidades que enfrentan las empresas en la protección de sus activos digitales. En este sentido, las conclusiones obtenidas no solo orientan aspectos importantes para la inversión en ciberseguridad, sino que también brindan un marco sólido para respaldar la toma de decisiones a nivel corporativo.

Uno de los aspectos clave que emerge del trabajo realizado es la necesidad de adoptar un enfoque integral de ciberseguridad. Esto implica reconocer que la protección efectiva contra las amenazas cibernéticas va más allá de la implementación de soluciones tecnológicas, y requiere una combinación de medidas técnicas, procesos de gestión de riesgos y concientización del personal. En este sentido, la inversión en tecnologías de seguridad avanzadas es fundamental, pero debe complementarse con programas de capacitación y concientización para el personal, así como el diseño de políticas y procedimientos robustos de gestión de riesgos.

Es vital para la organización evitar sanciones legales y salvaguardar su reputación cumpliendo con las regulaciones y normativas sobre protección de datos y privacidad. Es por esto, por lo que se enfatiza la necesidad de realizar actividades de hacking ético de manera responsable y dentro del marco legal establecido, asegurando así la integridad y la legitimidad de las pruebas de seguridad realizadas.

Todo esto que se relaciona, es con el fin de proporcionar una guía valiosa para que las organizaciones que buscan mejorar su postura de ciberseguridad puedan justificar la necesidad de inversión en este ámbito. Al adoptar un enfoque integral que abarque aspectos técnicos, legales y de gestión, así como al invertir en equipos especializados y en la ejecución de pruebas de intrusión, las organizaciones pueden fortalecer su resiliencia ante las crecientes amenazas cibernéticas y proteger sus activos digitales de manera efectiva.

La inversión en ciberseguridad no solo es una medida preventiva, sino también una inversión estratégica que contribuye a salvaguardar el éxito y la reputación de la organización en un entorno digital cada vez más complejo y desafiante.

7 CONCLUSIONES

Después de desplegar estrategias relacionadas con RedTeam & BlueTeam y observar su impacto en el desarrollo del informe, se concluye que la combinación de pruebas de penetración, medidas de remediación y endurecimiento ha contribuido significativamente a fortalecer la seguridad del sistema. Se destaca la importancia de mantener una vigilancia continua y realizar actualizaciones periódicas para adaptarse a las cambiantes amenazas cibernéticas y garantizar la protección integral de la infraestructura TI.

El aprendizaje continuo y las pruebas sobre los procesos técnicos dimensionados dentro de los marcos legales son esenciales para comprender el rol de las actividades dentro de las áreas de seguridad y sus funciones en el entorno.

8 RECOMENDACIONES

- Establecer un ciclo de evaluación continua de riesgos y vulnerabilidades, así como la implementación de medidas proactivas de seguridad, como la capacitación regular del personal en prácticas seguras de TI, específicamente enfocadas en las actividades de RedTeam & BlueTeam.

- Se aconseja realizar auditorías de seguridad periódicas en la infraestructura TI, implementar parches de seguridad de forma oportuna y utilizar herramientas avanzadas de detección de intrusiones específicamente adaptadas para las operaciones de RedTeam & BlueTeam.

- Se insta a establecer políticas claras de gestión de incidentes, con un enfoque especial en las actividades de RedTeam & BlueTeam, para garantizar una rápida detección y mitigación de cualquier brecha de seguridad que pueda surgir durante las pruebas de penetración.

- Se recomienda realizar evaluaciones periódicas de seguridad específicamente dirigidas a identificar y mitigar posibles puntos débiles en la infraestructura que puedan ser explotados durante las actividades.

- Se sugiere implementar medidas de parcheo regular y políticas de endurecimiento específicamente diseñadas para fortalecer la seguridad de los sistemas y satisfacer las necesidades de RedTeam & BlueTeam.

- Se aconseja utilizar herramientas de análisis de vulnerabilidades adaptadas a las actividades de RedTeam & BlueTeam para identificar y priorizar las amenazas potenciales de manera más efectiva, y establecer un proceso de gestión de parches eficiente.

ANEXOS

- LINK DEL VIDEO

https://youtu.be/87pyy9zQ5lE

BIBLIOGRAFÍA

1. Data, Protected. Protección de Datos. (2023). Disponible en: https://www.dataprotected.com.co/faq-proteccion-datos
2. Diario Oficial, LEY 1273 DE 2009. (2009). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
3. RedHat, El concepto de CVE. (2021). Foro y comunidad, Disponible en: https://www.redhat.com/es/topics/security/what-is-cve
4. Redacción, KeepCoding. ¿Qué es ExploitDB?. (2022). Tech School, Disponible en: https://keepcoding.io/blog/que-es-exploitdb/
5. Nowak, Shirly. ¿Qué es Pentesting?. (2022). nuclio digital school, Disponible en: https://nuclio.school/que-es-el-pentesting/#Que-fases-tiene-el-Pentesting
6. Diario Oficial, LEY 1273 DE 2009. (2009). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
7. Data, Protected. Protección de Datos. (2023). Disponible en: https://www.dataprotected.com.co/faq-proteccion-datos
8. COPNIA. Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (2022). Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
9. Portafolio, Ataque informático a Sanitas no comprometió información de usuarios. (2022). Disponible en: https://www.portafolio.co/negocios/empresas/eps-sanitas-detalles-del-ciberataque-que-sufrio-grupo-keralty-575968
10. Adastra. Conceptos Basicos de Meterpreter – MetaSploit Framework. (2022). thehackerway. Disponible en:

https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/

11. Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2
12. 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
13. Parra, Francis. ¿Qué hacer en caso de un ciberataque? (2020). Netdata. Disponible en: https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque
14. Australian, Government. Hardening Microsoft Windows 10 version 21H1 Workstations. (2021). v2, pg [6-49]. Disponible en: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Hardening%20Microsoft%20Windows%2010%20version%2021H1%20Workstations%20%28October%202021%29.pdf
15. UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?. (2020). Ingeniería y Tecnología. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/
16. Manage Engine. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)? (2023). Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html
17. Arnal, Carlos. ¿Cuál es la diferencia entre XDR y SIEM? (2023). WatchGuard. Disponible en: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem

18. Cody, Wilson. Evaluating the Efficacy of Network Forensic Tools: A Comparative Analysis of Snort, Suricata, and Zeek in Addressing Cyber Vulnerabilities. (2024). SANS. Disponible en: https://www.sans.org/white-papers/evaluating-efficacy-of-network-forensic-tools-comparative-analysis-snort-suricata-zeek-addressing-cyber-vulnerabilities/
19. García, Jorge. Políticas de seguridad: Por qué son importantes para tu negocio. (2024). deltaprotect. Disponible en: https://www.deltaprotect.com/blog/politicas-de-seguridad