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

MISHELL KARINA ROJAS MONTEALEGRE

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

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

MISHELL KARINA ROJAS MONTEALEGRE

JOHN FREDDY QUINTERO
TUTOR DE CURSO

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

Resumen

se abordaron múltiples aspectos relacionados con la ciberseguridad y la protección de datos en Colombia. Comienza examinando la legislación colombiana, en particular las leyes 1273 de 2009 y 1581 de 2012, que establecen normativas sobre la seguridad de los datos y los delitos informáticos. Se proporciona información detallada sobre las sanciones previstas y la entidad encargada de hacer cumplir estas leyes. Además, se resalta la importancia de llevar a cabo evaluaciones de seguridad y se enfoca en la ética en el ámbito de la ciberseguridad. También se analizan casos de cibercrimen para comprender mejor las amenazas. Asimismo, se subraya la necesidad de una respuesta efectiva frente a amenazas cibernéticas, haciendo hincapié en la configuración de firewalls y la implementación de registros de auditoría. Para terminar, este documento enfatiza la relevancia de cumplir con la legislación vigente, mantener altos estándares éticos y estar preparados para enfrentar desafíos en constante evolución en el entorno digital.

Tabla de contenido

Tabla de ilustraciones

Lista de tablas

Glosario

- **Superintendencia de Industria y Comercio (SIC):** Una entidad encargada de supervisar y hacer cumplir la ley de protección de datos personales en Colombia, con funciones que incluyen la vigilancia, investigación y sanción de infracciones.

- **Hábeas Data:** Derecho que garantiza a las personas el control y la protección de sus datos personales.

- **Pentesting (Test de Penetración**): Una evaluación de seguridad que simula un ataque cibernético para identificar vulnerabilidades en un sistema y mejorar la seguridad.

- **CVE (Glosario de Vulnerabilidades y Exposiciones Comunes):** Un identificador único asignado a vulnerabilidades de seguridad en software y sistemas.

- **Exploit Database (Exploit-DB**): Una plataforma en línea que proporciona exploits y detalles técnicos relacionados con vulnerabilidades conocidas.

- **Ley 1581 de 2012:** Una ley colombiana que regula la protección de datos personales y establece los derechos y responsabilidades relacionados con el tratamiento de información personal.

- **Datos Sensibles:** Información personal que se refiere a aspectos privados de la vida de una persona, como su salud, orientación sexual, creencias religiosas, entre otros.

- **Registro Nacional de Bases de Datos:** Un registro público en Colombia donde las entidades deben registrar sus bases de datos que contienen información personal, como parte de su cumplimiento con la Ley 1581.

- **COPNIA:** El Consejo Profesional Nacional de Ingeniería (COPNIA) es la entidad encargada de supervisar la ética y el cumplimiento de normas profesionales para los ingenieros en Colombia.

- **Código de Ética:** Un conjunto de principios y normas que rigen la conducta ética de una profesión o grupo profesional.

- **Cibercrimen:** Delitos o actividades ilegales realizadas en el ámbito cibernético, que incluyen el acceso no autorizado a sistemas, el robo de datos personales, el fraude en línea y más.

- **Ejercicio de Red Team:** Una simulación de ataque cibernético autorizado en la que un equipo de seguridad evalúa la resistencia de una organización a las amenazas cibernéticas.

- **Amenazas Cibernéticas:** Riesgos y peligros relacionados con la seguridad en línea que pueden afectar a una organización, como ataques de hackers, malware y ciberataques.

- **Ingeniería Social:** Técnicas utilizadas para manipular a las personas y obtener información confidencial, como contraseñas, a través de la interacción social.

- **Escaneo de Red:** Proceso de exploración de una red para identificar dispositivos y servicios disponibles.

- **Vulnerabilidad:** Una debilidad en un sistema o aplicación que puede ser explotada por un atacante para comprometer la seguridad.

- **Pruebas de Penetración:** Evaluación ética de sistemas y aplicaciones para identificar y explotar vulnerabilidades con el objetivo de fortalecer la seguridad.

- **Escalada de Privilegios:** Obtener un mayor nivel de acceso o control en un sistema comprometido, a menudo desde un nivel de usuario a un nivel de administrador.

- **DLL Hijacking:** Vulnerabilidad que permite a un atacante ejecutar código malicioso secuestrando archivos DLL.

- **Firewall:** Un sistema de seguridad que controla el tráfico de red para proteger una red o sistema contra amenazas no autorizadas.

- **Antivirus:** Software diseñado para detectar y eliminar malware y otras amenazas cibernéticas.

- **Acceso Remoto:** La capacidad de acceder y controlar un sistema de forma remota desde otro lugar.

- **Metasploit:** Una herramienta de código abierto utilizada para desarrollar y ejecutar exploits contra sistemas vulnerables.

- **Parches de Seguridad:** Actualizaciones diseñadas para corregir vulnerabilidades y mejorar la seguridad de un sistema o software.

Introducción

Este documento abarca múltiples etapas relacionadas con la ciberseguridad y la protección de datos en Colombia. Se inicia con un enfoque en la legislación colombiana, incluyendo la Ley 1273 de 2009 y la Ley 1581 de 2012, que regulan la protección de datos personales y los delitos informáticos. Se detallan las multas y la entidad encargada de su regulación. Además, se explora la importancia de las evaluaciones de seguridad, la ética en la ciberseguridad y se analizan incidentes de cibercrimen. También se destaca la necesidad de una respuesta eficaz ante amenazas cibernéticas, con un enfoque en la configuración de firewalls y la implementación de registros de auditoría. Estas etapas subrayan la importancia de cumplir con la legislación, mantener altos estándares éticos y estar preparados para enfrentar amenazas cibernéticas en un entorno digital en constante evolución.

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

- Recopilar los datos obtenidos sobre el escenario HackerHouse.
- Listar los eventos encontrados y dar las sugerencias al respecto.
- Explicar la importancia de los equipos de blueteam y redteam y de las políticas de seguridad.
- Sustentar el trabajo realizado dentro del curso mediante un video.

Desarrollo del informe

2 Etapa 1 conceptos

Ley 1273 de 2009[1]

Artículo 1. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

Capitulo primero

Artículo 269A. Acceso abusivo a un sistema informático: Acceder ilegalmente a un sistema informático protegido, permanecer sin permiso o contra la voluntad del legítimo usuario, resultará en una pena de prisión de 48 a 96 meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación. Quien interfiera ilegalmente con el funcionamiento de un sistema informático, acceso a datos o red de telecomunicaciones, enfrentará prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos, a menos que la acción sea un delito con pena mayor.

Artículo 269C. Interceptación de datos informáticos. Quien sin orden judicial intercepte datos informáticos en su origen, destino o sistema, o las emisiones electromagnéticas de un sistema informático, enfrentará prisión de 36 a 72 meses.

Artículo 269D. Daño informático. Destruir, dañar, alterar o suprimir datos o sistemas informáticos sin autorización resultará en prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. Uso de software malicioso. Producir, traficar, distribuir o poseer software malicioso sin autorización conlleva prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F. Violación de datos personales. Obtener, divulgar o usar indebidamente datos personales sin autorización, para beneficio propio o de otros,

[1] Colombia, R. d. (5 de Enero de 2009). [Sitio Web]. SIC. Obtenido de LEY 1273 DE 2009 [consultado el 07 de Octubre 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

resultará en prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. Suplantación de sitios web para capturar datos personales. Diseñar, desarrollar, traficar o enviar contenido web ilícito sin autorización conlleva pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes, a menos que sea un delito más grave. Modificar el sistema de nombres de dominio para engañar al usuario también resultará en la misma pena, agravada hasta la mitad si hay reclutamiento de víctimas en la cadena del delito.

Artículo 269H. Circunstancias de agravación punitiva: Las penas por conductas descritas en este título se incrementarán de la mitad a tres cuartas partes en el siguiente caso:

establece que cometer acciones en redes estatales o financieras, realizadas por servidores públicos en ejercicio, con intención de aprovechar la confianza, divulgar información perjudicial, obtener beneficios o fines terroristas, incluso utilizando a terceros inocentes, puede acarrear sanciones. Si el responsable controla la información, podría enfrentar hasta tres años de inhabilitación en campos vinculados a sistemas informáticos. También se considera un delito obtener ganancias para uno mismo o para otros, con objetivos terroristas o amenazando la seguridad nacional, empleando a terceros confiables. Además, si quien lleva a cabo estas acciones tiene responsabilidad en la administración, manejo o control de la información, podría ser inhabilitado hasta tres años para ejercer profesiones relacionadas con sistemas de información procesada con equipos computacionales.

Capitulo segundo

De los atentados informáticos y otras infracciones

Artículo 2691. Hurto por medios informáticos y semejantes. Quien, al sortear medidas de seguridad informática, realice la acción descrita en el artículo 239 mediante manipulación de sistemas informáticos o suplantación de usuario en sistemas de autenticación, enfrentará las sanciones del artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. Quien, buscando beneficio económico, utilice manipulación informática u otros métodos similares para lograr la transferencia no autorizada de activos perjudicando a otro, enfrentará prisión de 48 a 120 meses y multa de 200 a 1500 salarios mínimos legales mensuales vigentes, salvo delito más grave. Esta misma pena se aplica a quienes creen, posean o faciliten programas informáticos para cometer este delito o una estafa. Si el monto involucrado excede 200 salarios mínimos, la sanción se incrementa en la mitad.

Artículo 2. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Articulo 58 Circunstancias de mayor punibilidad. Las circunstancias de mayor punibilidad incluyen el uso de medios informáticos, electrónicos o telemáticos para cometer los delitos, a menos que ya estén contemplados de otra manera.

Ley 1581 de 2012[2]

Objeto, ámbito de aplicación y definiciones

Artículo 1. El propósito de esta ley es establecer y garantizar el derecho de todas las personas a acceder, rectificar y mantener actualizada la información que les concierne en bases de datos y archivos. Además, busca salvaguardar otros derechos y libertades constitucionales, en particular el derecho a la información, como lo estipula la Constitución Política, particularmente en sus artículos 15 y 20.

Artículo 2. Esta ley abarca datos personales en bases de datos de entidades públicas o privadas. Se aplica dentro de Colombia y también a tratamientos extraterritoriales sujetos a legislación colombiana por acuerdos internacionales. Excluye bases de datos personales en ámbito doméstico, seguridad nacional, lavado de activos, inteligencia, información periodística, entre otras. Los elementos de protección de datos aplican a todas las bases, respetando limitaciones y reservas legales. Si leyes especiales rigen bases excluidas, sus principios también se aplican junto con los de esta ley.

Artículo 3. Conceptos fundamentales en esta ley incluyen:

- **Autorización:** La aprobación previa, informado y expreso otorgado por el Titular para acceder el tratamiento de sus datos personales.
- **Base de Datos:** Un ligado organizado de datos personales que están sujetos a ser procesados.
- **Dato personal**: La información propia a una persona natural identificable, permitiendo su identificación directa o indirecta.
- **Encargado del Tratamiento:** Persona o entidad que trata datos por cuenta del Garante.
- **Responsable del Tratamiento:** Persona o entidad que concluye sobre el tratamiento de los datos.
- **Titular:** Persona natural cuyos datos se tratan.

[2] publica, D. a. (18 de Octubre de 2012) . [Sitio Web]. Funcion Publica. Obtenido de Ley 1581 de 2012. . [consultado el 07 de Octubre 2023]. Diponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

- **Tratamiento:** Ordenamientos sobre datos, como recolección, provisión, uso y supresión.

Principios rectores

Artículo 4. Principios fundamentales para el tratamiento de datos personales son:

- **Legalidad:** El tratamiento debe cumplir la ley y regulaciones aplicables.
- **Finalidad:** Debe tener una razón legítima y comunicarse al titular.
- **Consentimiento:** Requiere autorización previa, informada y expresa del titular, salvo mandato legal o judicial.
- **Veracidad:** Los datos deben ser precisos, completos y actualizados, evitando información engañosa.
- **Transparencia:** El titular puede solicitar información sobre sus datos en cualquier momento.
- **Acceso restringido:** El tratamiento se limita a personas autorizadas; datos privados no pueden estar públicamente disponibles en Internet.
- **Seguridad:** Se deben implementar medidas técnicas y administrativas para proteger los datos.
- **Confidencialidad:** Quienes participen en el tratamiento deben mantener la reserva de la información, incluso después de su relación con el proceso de tratamiento.

Categorías especiales de datos

Artículo 5. Según los términos de esta ley, los datos sensibles abarcan información que involucra la privacidad del titular y cuyo uso inapropiado podría resultar en discriminación. Estos datos incluyen aspectos como el origen étnico, las creencias, las afiliaciones políticas, el estado de salud, la vida sexual y los datos biométricos. La protección de estos tipos de datos es de especial importancia para preservar la dignidad y la igualdad de las personas en diversos contextos.

Artículo 6. El tratamiento de datos sensibles está prohibido, excepto en casos de:

- Autorización explícita del titular, a menos que la ley no requiera autorización.
- Protección del interés vital del titular cuando esté incapacitado física o legalmente, con autorización de representantes legales.
- Actividades legítimas de organizaciones sin fines de lucro con objetivos políticos, filosóficos, religiosos o sindicales, solo para sus miembros o contactos regulares, sin divulgación a terceros sin consentimiento.
- Reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- Fines históricos, estadísticos o científicos, tomando medidas para anonimizar a los titulares.

Artículo 7. Los derechos de niños y adolescentes en el manejo de datos están asegurados. Solo se pueden usar sus datos si son públicos. El Estado y las escuelas deben educar a padres sobre los riesgos de un mal uso de datos y fomentar el uso seguro de la información de los menores. El Gobierno regulará esto en seis meses tras la ley.

Derechos y condiciones de legalidad para el tratamiento de datos

Artículo 8. Los titulares de datos personales tienen los siguientes derechos:

- Conocer, actualizar y corregir sus datos ante los responsables del tratamiento.
- Pedir prueba de la autorización dada, salvo excepciones legales.
- Solicitar información sobre el uso dado a sus datos por los responsables o encargados del tratamiento.
- Presentar quejas ante la Superintendencia de Industria y Comercio por violaciones a la ley.
- Revocar autorizaciones y solicitar eliminación de datos si no se respetan principios y garantías legales, en caso de comprobada infracción.
- Acceder gratuitamente a sus datos tratados.

Artículo 9. Se requiere obtener el consentimiento previo e informado del titular para llevar a cabo el procesamiento de datos, a menos que se apliquen excepciones legales. Es esencial que esta autorización sea adquirida de manera que sea referenciable en el tiempo futuro.

Artículo 10. No se necesita autorización del titular en los siguientes casos:

La obligación de cumplir con las disposiciones de esta ley es necesaria al acceder a datos personales sin autorización, en situaciones que incluyen la información requerida por entidades públicas o judiciales en ejercicio de sus funciones, datos de naturaleza pública, urgencias médicas o sanitarias, tratamientos permitidos por la ley con fines históricos, estadísticos o científicos, y datos del Registro Civil de las Personas.

Artículo 11. La información requerida por el titular puede ser proporcionada en cualquier medio, incluso electrónicamente, de manera fácil de leer y sin obstáculos técnicos. Debe coincidir completamente con la almacenada en la base de datos.

El Gobierno Nacional definirá cómo los responsables y encargados del tratamiento deben suministrar esta información, considerando la naturaleza de los datos personales. Esta regulación se establecerá en el año siguiente a la promulgación de la ley.

Artículo 12. El responsable del Tratamiento debe informar claramente al titular al solicitar la autorización, proporcionando lo siguiente:

- Descripción del tratamiento de sus datos y su propósito.
- Opcionalidad de responder a preguntas relacionadas con datos sensibles o datos de menores.
- Los derechos del titular.
- Identificación, dirección y contacto del responsable del Tratamiento.

El responsable debe guardar evidencia de este cumplimiento y, si el titular lo solicita, proporcionarle una copia.

Artículo 13. La información que se ajuste a los criterios definidos por esta ley tiene la posibilidad de ser entregada a:

- Los titulares, así como también a sus herederos o representantes legales.
- Entidades públicas o administrativas en concordancia con su mandato legal o por mandato judicial.
- Terceros debidamente autorizados por el titular o conforme a las normativas legales.

Procedimientos

Artículo 14. Los titulares o sus herederos tienen derecho a consultar su información personal en cualquier base de datos, pública o privada. El responsable o Encargado del Tratamiento debe proporcionar toda la información del registro individual o vinculada a la identificación del titular. La consulta se hará a través de los medios establecidos por ellos, con posibilidad de dejar constancia.
La consulta debe ser atendida en un plazo de hasta 10 días hábiles. Si no es posible cumplir en ese tiempo, se notificará al interesado con razones y nueva fecha, que no podrá exceder 5 días hábiles adicionales. En casos especiales, leyes o reglamentos podrían establecer plazos más cortos según la naturaleza de los datos.

Artículo 15. Los titulares o sus herederos pueden presentar reclamos sobre información incorrecta o incumplimiento de deberes ante el Responsable o Encargado del Tratamiento, siguiendo estas pautas:

- El reclamo se envía al Responsable o Encargado del Tratamiento, incluyendo detalles del titular y los hechos del reclamo. Si es incompleto, se solicita aclaración en 5 días. Si no se recibe información en 2 meses, se considera

como desistimiento. Si el receptor no es competente, lo remite en 2 días hábiles.
- Se agrega la leyenda "reclamo en trámite" en la base de datos en máximo 2 días hábiles, con motivo del reclamo, hasta su resolución.
- El reclamo se atiende en 15 días hábiles, extendibles a 8 días si se justifica demora. Se informa al interesado sobre razones y nueva fecha.

Artículo 16. Previo a presentar una queja ante la Superintendencia de Industria y Comercio, es necesario que el titular de los datos, o su heredero, complete el procedimiento de consulta o reclamo directamente con el Responsable o Encargado del Tratamiento.

Deberes de los responsables del tratamiento y encargados del tratamiento

Artículo 17. Los responsables del Tratamiento deben cumplir con los siguientes deberes, además de otras disposiciones de la ley:

- Garantizar el ejercicio del derecho de hábeas data del Titular en todo momento.
- Solicitar y conservar copias de las autorizaciones otorgadas por el Titular.
- Informar al Titular sobre la finalidad de la recolección y sus derechos.
- Mantener seguridad de la información para evitar su alteración, pérdida o acceso no autorizado.
- Garantizar la veracidad, integridad y actualización de los datos suministrados al Encargado del Tratamiento.
- Actualizar y corregir la información incorrecta ante el Encargado del Tratamiento.
- Suministrar al Encargado solo los datos autorizados.
- Velar por la seguridad y privacidad de la información del Titular ante el Encargado del Tratamiento.
- Atender consultas y reclamos según lo establecido en la ley.
- Tener un manual interno para el cumplimiento de la ley, atención de consultas y reclamos.
- Informar al Encargado si cierta información está en disputa por parte del Titular.
- Informar al Titular sobre el uso de sus datos.
- Informar a la autoridad de protección de datos sobre violaciones de seguridad.
- Cumplir con instrucciones de la Superintendencia de Industria y Comercio.

Artículo 18. Los Encargados del Tratamiento deben cumplir los siguientes deberes, además de otras disposiciones de la ley:

- Garantizar el ejercicio del derecho de hábeas data del Titular en todo momento.
- Mantener seguridad de la información para evitar su alteración, pérdida o acceso no autorizado.
- Actualizar, corregir o eliminar datos según lo establecido en la ley.
- Actualizar la información reportada por los Responsables del Tratamiento en un plazo de cinco días hábiles.
- Atender consultas y reclamos de los Titulares según lo establecido en la ley.
- Tener un manual interno para el cumplimiento de la ley y atención de consultas y reclamos.
- Registrar la leyenda "reclamo en trámite" en la base de datos.
- Insertar la leyenda "información en discusión judicial" cuando notificado por la autoridad competente.
- No circular información controvertida por el Titular y bloqueada por la Superintendencia.
- Limitar el acceso a la información solo a quienes tengan autorización.
- Informar a la Superintendencia sobre violaciones a códigos de seguridad y riesgos en la administración de información de los Titulares.
- Cumplir instrucciones de la Superintendencia de Industria y Comercio.
- En caso de que la misma persona sea Responsable y Encargado del Tratamiento, debe cumplir ambos conjuntos de deberes.

De los mecanismos de vigilancia y sanción

Artículo 19. La Superintendencia de Industria y Comercio supervisará el cumplimiento de la ley de protección de datos personales a través de una Delegatura para la Protección de Datos Personales. El Gobierno establecerá una estructura dentro de la Superintendencia para ejercer estas funciones en un plazo de seis meses. La vigilancia de los datos personales regulados por la Ley 1266 de 2008 seguirá las disposiciones de dicha norma.

Artículo 20. La Superintendencia de Industria y Comercio dispondrá de los recursos asignados en el Presupuesto General de la Nación para llevar a cabo sus funciones según esta ley.

Artículo 21. La Superintendencia de Industria y Comercio tiene diversas funciones, como supervisar el cumplimiento de las leyes de protección de datos, llevar a cabo investigaciones y asegurar el derecho de hábeas data, bloquear temporalmente

datos en caso de riesgo para los derechos, promover los derechos relacionados con el tratamiento de datos y emitir declaraciones para transferencias internacionales. También administra el Registro Nacional Público de Bases de Datos, sugiere ajustes normativos y solicita colaboración de entidades extranjeras en casos relevantes. Además, realiza otras tareas designadas por la ley.

Artículo 22. La Superintendencia de Industria y Comercio, al identificar incumplimientos de esta ley por parte de Responsables o Encargados del Tratamiento, tomará medidas y aplicará sanciones. En casos no contemplados por esta ley, se seguirán las normas del Código Contencioso Administrativo.

Artículo 23. La Superintendencia de Industria y Comercio cuenta con la autoridad para implementar penalizaciones a los Responsables y Encargados del Tratamiento de datos. Estas penalidades abarcan multas tanto a nivel individual como institucional, la suspensión temporal de actividades relacionadas con el manejo de datos, la clausura temporal de operaciones y, en situaciones involucrando datos sensibles, el cierre inmediato y definitivo de las actividades. Es importante destacar que estas medidas sancionadoras son aplicables a entidades privadas. En el caso de incumplimientos provenientes de entidades públicas, la Superintendencia remitirá el asunto a la Procuraduría General de la Nación para llevar a cabo una investigación.

Artículo 24. Las sanciones por infracciones a la ley se graduarán teniendo en cuenta varios criterios, cuando sean aplicables:

- La magnitud del daño o riesgo a los intereses protegidos por la ley.
- El lucro obtenido por el infractor o terceros debido a la infracción.
- La reincidencia en la comisión de la infracción.
- La resistencia, negativa u obstrucción a la investigación o supervisión de la Superintendencia.
- La negativa o desobediencia a las órdenes de la Superintendencia.
- La admisión de culpa por parte del infractor antes de la imposición de la sanción correspondiente.

Artículo 25. El Registro Nacional de Bases de Datos, bajo la supervisión de la Superintendencia de Industria y Comercio, es un repositorio público que alberga información acerca de las bases de datos sujetas a Tratamiento dentro del país. Este recurso es de libre acceso para todos los ciudadanos.

A fin de registrar bases de datos en este sistema, aquellos interesados en hacerlo deben suministrar a la Superintendencia sus políticas de tratamiento de información. Estas políticas, que serán de carácter obligatorio para los responsables y encargados del Tratamiento, deben cumplirse. El incumplimiento de estas políticas

conllevará a la aplicación de sanciones. Cabe mencionar que estas políticas deben ser, al menos, igual de rigurosas que los deberes establecidos por la ley.
En un plazo de un año a partir de la promulgación de la ley, el Gobierno Nacional establecerá regulaciones que detallarán aspectos del Registro, tales como la información esencial que se requiere y los términos para la inscripción de los Responsables del Tratamiento.

Artículo 26. La transferencia de datos personales a países que no cumplan con niveles adecuados de protección según los estándares de la Superintendencia de Industria y Comercio está prohibida, los cuales deben ser iguales o superiores a los establecidos por la ley. Existen excepciones a esta prohibición en determinadas situaciones:

- Cuando el Titular haya otorgado autorización expresa e inequívoca para la transferencia.
- En el caso de intercambio de datos médicos por razones de salud pública.
- Para transferencias bancarias o bursátiles según la legislación aplicable.
- En acuerdos de transferencia en tratados internacionales en los que Colombia participe.
- Cuando la transferencia sea necesaria para cumplir un contrato con el Titular o medidas precontractuales con su autorización.
- En transferencias legalmente exigidas para el interés público o para el ejercicio de derechos en procesos judiciales.

La Superintendencia de Industria y Comercio tendrá la facultad de emitir declaraciones de conformidad para transferencias internacionales de datos y podrá requerir información y realizar investigaciones para verificar el cumplimiento de los requisitos.

Estas disposiciones se aplican a todos los datos personales, incluyendo los contemplados en la Ley 1266 de 2008.

Artículo 27. El Gobierno Nacional emitirá regulaciones para establecer Normas Corporativas Vinculantes que certifiquen las buenas prácticas en protección de datos personales y su transferencia a terceros países.

Artículo 28. Las personas que actualmente realizan actividades reguladas por esta ley tendrán un período de hasta seis (6) meses a partir de su entrada en vigencia para ajustarse a sus disposiciones.

Artículo 29. La presente ley anula todas las disposiciones que sean contrarias a ella, excepto aquellas especificadas en el artículo 2°.

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

¿Qué es el Pentesting?

El Pentesting, o test de penetración, es una evaluación de seguridad informática que identifica posibles fallos en un sistema y su alcance. Combina "penetration" y "testing". Se simula un ataque cibernético para evaluar y superar los sistemas de seguridad de una organización. Los resultados se entregan en un informe para implementar mejoras y fortalecer la ciberseguridad. Es eficaz para evaluar defensas empresariales y mejorar la seguridad.[3]

Las cinco fases del Pentesting[4] son:

- Recopilación y planificación.
- Análisis de vulnerabilidades.
- Modelado de amenazas.
- Explotación del sistema.
- Elaboración de los informes.

Recopilación Y Planificación

La primera fase del Pentesting, también conocida como fase de planificación, es un componente crucial en la evaluación de la seguridad informática de una organización. En esta etapa, se establecen los cimientos para llevar a cabo un análisis exhaustivo y detallado de la infraestructura de TI y los sistemas de seguridad de una empresa. A continuación, se detallan los principales aspectos de esta fase:

- **Definición de Objetivos:** En esta etapa inicial, se trabajará en estrecha colaboración con la empresa para establecer claramente los objetivos y alcance del Pentesting. Esto puede incluir determinar qué sistemas

[3] NOWAK, S. (28 de Noviembre de 2022). [Sitio Web]. nuclio. Obtenido de ¿Qué es el Pentesting? [consultado el 07 de Octubre 2023]. Disponible en: https://nuclio.school/que-es-el-pentesting/

[4] Hernández, M. (21 de Marzo de 2022). [Sitio Web]. ciberseguridad bidaidea. Obtenido de ¿Cuál son la 5 Fases del Pentesting? [consultado el 07 de Octubre 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

específicos serán evaluados, cuáles son las áreas críticas de enfoque y qué se espera lograr con el ejercicio de prueba de penetración.

- **Selección de Sistemas y Métodos:** Se identifican los sistemas, redes o aplicaciones que serán sometidos al Pentesting. Esta selección puede basarse en la importancia estratégica de los activos, la probabilidad de vulnerabilidades y la exposición al riesgo. Además, se definen los métodos y técnicas que se utilizarán durante el proceso de evaluación, como pruebas de intrusión externa o interna, análisis de vulnerabilidades, explotación de brechas, entre otros.

- **Recopilación de Datos:** En esta fase, se recolecta información relevante sobre la organización, sus sistemas, redes, infraestructura y empleados. Esto puede incluir detalles técnicos sobre servidores, puertos abiertos, direcciones IP, dominios, información de contacto, estructura de red y otros datos relevantes. La recopilación de información es esencial para comprender el entorno de seguridad y planificar de manera efectiva el Pentesting.

- **Técnicas de Recopilación**: La recopilación de datos puede involucrar una variedad de técnicas y herramientas. Esto puede incluir escaneos de IP y puertos para identificar puntos de entrada posibles, obtención de metadatos de documentos y archivos expuestos en línea, búsqueda de información sensible a través de técnicas de Google Hacking o Dorking, y el uso de herramientas como Nmap para descubrir dispositivos en una red o SubFinder para encontrar subdominios.

- **Preparación del Entorno:** Además de la recopilación de datos, esta fase también puede implicar la preparación del entorno de Pentesting. Esto podría incluir la configuración de sistemas de prueba, la instalación de herramientas y software necesarios, y la creación de un entorno aislado y seguro donde se llevarán a cabo las pruebas.

Análisis De Vulnerabilidades

En la segunda fase del Pentesting, conocida como la fase de exploración y análisis, se profundiza en la evaluación de la seguridad de los sistemas de una organización. Esta etapa es esencial para descubrir las debilidades potenciales y evaluar la efectividad de las defensas cibernéticas ante un posible ataque. A continuación, se proporciona una ampliación de esta fase:

- **Simulación de Intrusión:** En esta etapa, los expertos en seguridad cibernética intentarán replicar las tácticas de un atacante real. A través de una serie de pruebas controladas, se simulan posibles métodos de intrusión

que un atacante podría utilizar para acceder a la red, sistemas o aplicaciones de la organización.

- **Identificación de Puntos Débiles:** Se realizan pruebas activas y pasivas para identificar y explorar vulnerabilidades en los sistemas. Las pruebas activas pueden incluir el uso de herramientas de escaneo de vulnerabilidades para identificar debilidades conocidas en la infraestructura. Las pruebas pasivas implican el monitoreo de la red para identificar información sensible que se esté transmitiendo sin cifrado o cualquier otra actividad sospechosa.

- **Análisis de Vulnerabilidades:** Los resultados de las pruebas se analizan minuciosamente para evaluar la gravedad de las vulnerabilidades identificadas y su impacto potencial en la seguridad de la organización. Esto permite a los expertos en seguridad priorizar las vulnerabilidades según su nivel de riesgo y potencial de explotación.

- **Evaluación de Escenarios de Ataque:** Los especialistas en seguridad cibernética pueden crear y evaluar diversos escenarios de ataque para comprender cómo podrían ser explotadas las vulnerabilidades identificadas. Esto ayuda a la organización a comprender mejor las posibles consecuencias de una intrusión y a tomar medidas proactivas para mitigar los riesgos.

- **Determinación del Alcance Definitivo:** Basándose en los resultados obtenidos en la fase de exploración y análisis, se puede refinar y definir definitivamente el alcance del Pentesting. Esto implica establecer qué sistemas, aplicaciones o áreas específicas serán objeto de pruebas adicionales y cómo se abordarán las debilidades identificadas.

- **Generación de Informe Intermedio:** A medida que se realizan pruebas y se obtienen resultados, se puede generar un informe intermedio que destaque las vulnerabilidades críticas encontradas hasta el momento. Esto permite a la organización tomar medidas iniciales para abordar las amenazas más urgentes antes de que finalice el Pentesting completo.

Modelado De Amenazas

En la tercera fase del Pentesting, conocida como la fase de explotación y modelado de amenazas, se lleva a cabo la ejecución controlada de ataques dirigidos a las vulnerabilidades previamente identificadas en la infraestructura de una organización. Esta etapa es esencial para comprender cómo podrían ser explotadas las debilidades y evaluar la capacidad del sistema para defenderse contra amenazas reales. A continuación, se proporciona una expansión de esta fase:

- **Desarrollo de Escenarios de Ataque**: En esta etapa, los expertos en seguridad cibernética diseñan y desarrollan escenarios de ataque específicos basados en las vulnerabilidades detectadas. Estos escenarios pueden incluir técnicas de explotación como inyecciones SQL, ataques de fuerza bruta, manipulación de sesiones y otros métodos que un atacante real podría emplear.

- **Ejecución Controlada de Ataques:** Los especialistas en seguridad cibernética implementan los escenarios de ataque diseñados en entornos controlados y aislados, asegurándose de no causar daño real a los sistemas de la organización. Durante esta fase, se monitorizan de cerca las respuestas del sistema ante los ataques y se registran los resultados obtenidos.

- **Modelado de Amenazas y Evaluación de Respuestas:** A medida que se realizan los ataques controlados, se evalúa cómo el sistema responde a cada uno de ellos. Se observa si las defensas cibernéticas son capaces de detectar, bloquear o mitigar eficazmente los ataques. Esta información permite modelar las posibles amenazas y entender cómo podrían afectar a la organización en un entorno real.

- **Identificación de Rutas de Acceso y Propagación:** En algunos casos, los ataques exitosos podrían proporcionar a los expertos en seguridad cibernética acceso a sistemas internos o áreas sensibles de la red. Esto permite evaluar la facilidad con la que un atacante podría moverse lateralmente y propagar su presencia en la infraestructura.

- **Recopilación de Evidencia:** Durante la ejecución de los ataques, se recopila información detallada sobre cómo se llevaron a cabo y los resultados obtenidos. Esta evidencia será esencial para respaldar las recomendaciones y conclusiones que se incluirán en el informe final.

- **Definición de Mejoras y Mitigaciones:** Basándose en los resultados de los ataques controlados y el modelado de amenazas, se identifican las áreas de mejora necesarias en la infraestructura de seguridad. Se proponen soluciones y recomendaciones específicas para mitigar las vulnerabilidades, fortalecer las defensas y reducir los riesgos de futuros ataques.

- **Generación de Informe Final:** Una vez concluida esta fase, se elabora un informe final detallado que documenta los escenarios de ataque, los resultados obtenidos, las vulnerabilidades explotadas y las recomendaciones para mejorar la ciberseguridad. Este informe proporciona a la organización una visión clara de las áreas críticas que requieren atención y cómo abordarlas de manera efectiva.

Explotación Del Sistema

La fase de simulación de ataques es uno de los componentes fundamentales en un proceso de Pentesting, donde se diseñan y ejecutan escenarios de ataque controlados con el fin de evaluar la ciberseguridad de un sistema o red. Esta etapa busca evaluar las amenazas potenciales, analizar cómo el sistema responde ante los ataques y proporcionar al propietario una comprensión precisa de las vulnerabilidades existentes. A continuación, se expande sobre esta fase clave del Pentesting:

- **Simulación de Ataques y Evaluación de Amenazas:** Diseño de Escenarios de Ataque: Los expertos en seguridad cibernética desarrollan escenarios de ataque específicos basados en las vulnerabilidades previamente identificadas. Estos escenarios representan posibles métodos que un atacante podría utilizar para explotar debilidades en el sistema.

- **Ejecución de Ataques Controlados**: Se implementan los escenarios de ataque diseñados en entornos controlados, siguiendo estrictos protocolos para evitar daños reales a los sistemas. Durante esta fase, se realizan pruebas en busca de vulnerabilidades como inyecciones de código, fallos de autenticación, vulnerabilidades de configuración y otros vectores de ataque.

- **Evaluación de Respuestas del Sistema:** A medida que se ejecutan los ataques controlados, se observa cómo el sistema responde a cada uno de ellos. Se evalúa la detección, bloqueo y mitigación de los ataques por parte de las defensas cibernéticas. Esta evaluación ayuda a entender las capacidades de respuesta del sistema frente a amenazas reales.
- **Explotación de Vulnerabilidades:** Los escenarios de ataque se ejecutan para explotar las vulnerabilidades detectadas y se analiza si los ataques tienen éxito. Esto proporciona una comprensión práctica de cómo podrían ser utilizadas las vulnerabilidades para comprometer la seguridad del sistema.

- **Afinamiento de Defensas:** En algunos casos, durante la simulación de ataques, los especialistas en seguridad cibernética pueden llevar al límite las defensas del sistema para comprender sus puntos débiles y ajustarlas de manera más efectiva. Esto implica probar diferentes técnicas de ataque y ajustar los parámetros de seguridad para mejorar la detección y respuesta a amenazas.

Información Y Reporte

Una vez finalizada esta fase, se recopilan datos detallados sobre los ataques realizados y sus resultados. Estos datos se utilizan para generar un informe

completo que describe los escenarios de ataque, las vulnerabilidades explotadas, los hallazgos clave y las recomendaciones para mejorar la ciberseguridad. Este informe es esencial para que el propietario del sistema comprenda las áreas vulnerables y tome medidas adecuadas para mitigar los riesgos.

¿Qué herramientas se utilizan para el pentesting?

El Pentesting se apoya en diversas herramientas informáticas para cada una de sus fases, optimizando así la detección y evaluación de vulnerabilidades. Algunas de estas herramientas incluyen:

- **Nmap, Dnsrecon y SubFinder:** Escanean sistemas, dominios y puertos para identificar posibles vulnerabilidades y puntos débiles.
- **BurpSuite:** Realiza un análisis en profundidad de sistemas y sitios web, identificando posibles fallos de seguridad.
- **Nessus:** Realiza análisis exhaustivos y compara con bases de datos para identificar vulnerabilidades.
- **Metasploit:** Permite llevar a cabo la explotación de vulnerabilidades detectadas, brindando un amplio alcance de pruebas.
- **John the Ripper:** Ayuda a descifrar contraseñas y claves encriptadas.
- **Veil:** Se utiliza para enmascarar código malicioso y evaluar la resistencia del sistema a ataques simulados.
- **Pentesting con Python:** Python se ha convertido en una opción popular para realizar Pentesting debido a su versatilidad y facilidad de uso. Las bibliotecas y módulos disponibles permiten la creación de scripts personalizados para realizar pruebas específicas y automatizar tareas de Pentesting. La flexibilidad de Python facilita la adaptación a diferentes situaciones y necesidades de seguridad.

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

El "footprinting" es una de las etapas más importantes dentro del pentesting debido a su papel fundamental en la planificación y ejecución exitosa de las pruebas de seguridad. Esta etapa se centra en la recopilación de información detallada sobre el objetivo del pentesting, como sistemas, redes, infraestructura, empleados y cualquier otra entidad relacionada. El footprinting permite a los pentesters entender completamente la infraestructura y la presencia en línea del objetivo. Esta información es esencial para diseñar un enfoque de pentesting efectivo y eficiente. La recopilación de información en la etapa de footprinting permite a los pentesters modelar posibles escenarios de ataque. Esto es crucial para simular ataques realistas que podrían llevarse a cabo por actores malintencionados.

- ✓ **Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux. Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:**

- **¿Qué es un CVE y su estructura?**
- **https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?**

CVE:[5] El Glosario de Vulnerabilidades y Exposiciones Comunes (CVE) es un proyecto de seguridad respaldado por la División de Seguridad Nacional de EE. UU. y gestionado por la Corporación MITRE. Su enfoque es el software de lanzamiento público y utiliza el Protocolo de Automatización de Contenido de Seguridad (SCAP) para recopilar información sobre vulnerabilidades y exposiciones de seguridad. Estas son catalogadas y asignadas a identificadores únicos.
Cada vulnerabilidad documentada recibe una identificación única por parte de MITRE. Pocos días después de ser publicadas en la base de datos de vulnerabilidades de MITRE, la Base de Datos Nacional de Vulnerabilidades (NVD) las publica junto con un análisis de seguridad.

El CVE, según la definición de MITRE, es un glosario o diccionario de vulnerabilidades y exposiciones disponibles al público. Su objetivo es proporcionar una referencia estándar para la industria, permitiendo la comunicación y discusión coherente sobre vulnerabilidades específicas. Esto facilita la interacción entre avisos de seguridad, rastreadores de errores y bases de datos alrededor de la misma vulnerabilidad, creando un "lenguaje común" para abordar estos temas en la comunidad de seguridad.

[5] ciberseguridad. (s.f.). [Sitio Web]. ciberseguridad. Obtenido de ¿QUÉ ES CVE? EXPLICACIÓN DE LAS VULNERABILIDADES Y EXPOSICIONES COMUNES [consultado el 07 de Octubre 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

Incorporación de una CVE[6]

El proceso de incorporación de una nueva vulnerabilidad al listado CVE consta de tres etapas:

- **Etapa de presentación inicial y tratamiento**: El CVE Content Team analiza y procesa las solicitudes de registro de nuevas vulnerabilidades. Se investiga y evalúa la información proporcionada.
- **Etapa de candidatura:** En esta fase, se asigna el CVE-ID, el identificador único. Puede ocurrir de tres maneras: asignación directa por el CVE Content Team, asignación directa por el CVE Editor en caso de vulnerabilidades críticas sin autor claro, o reserva de un CVE-ID por parte de organizaciones antes de hacer la propuesta.
- **Etapa de publicación en la lista (si es aceptada la candidatura):** Se agrega la entrada a la lista y se publica en el sitio web del diccionario CVE. Puede llevar tiempo debido a procesos de revisión y ajustes en la descripción o referencias.

Estas etapas explican por qué la lista CVE no incluye vulnerabilidades de día cero (recién descubiertas), ya que el proceso involucra análisis y verificación antes de su publicación.

Formato[7]

Los elementos de la lista CVE se identifican mediante formatos llamados CVE-ID, que siguen estas formas:

- **Para las entradas CVE:** CVE-YYYY-NNNN (YYYY representa el año y NNNN el número de la vulnerabilidad). Desde enero de 2014, el identificador puede tener más de cuatro dígitos si es necesario.
- **Para las entradas candidatas a CVE:** CAN-YYYY-NNNN (YYYY representa el año y NNNN el número de la vulnerabilidad).

[6] wikipedia. (12 de Julio de 2023). [Sitio Web]. wikipedia. Obtenido de Common Vulnerabilities and Exposures [consultado el 07 de Octubre 2023]. Disponible en: https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

[7] wikipedia. (12 de Julio de 2023). [Sitio Web]. wikipedia. Obtenido de Common Vulnerabilities and Exposures [consultado el 07 de Octubre 2023]. Disponible en: https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Exploit-DB[8]

Exploit Database (Exploit-DB) es una plataforma en línea que proporciona una amplia colección de exploits y vulnerabilidades para diferentes aplicaciones, sistemas operativos y dispositivos. Esta base de datos es una valiosa herramienta para investigadores de seguridad, profesionales de ciberseguridad y pentesters que desean acceder a exploits ya conocidos y sus detalles técnicos para fines de prueba y análisis.

A continuación, se describe cómo se utiliza Exploit Database:

- **Acceso a la Plataforma:** Visita el sitio web oficial de Exploit Database en https://www.exploit-db.com/.

- **Navegación:** Utiliza la barra de búsqueda o las categorías disponibles para explorar los exploits por tipo de software, sistema operativo o plataforma. Puedes buscar exploits por palabras clave, nombres de programas o nombres de fabricantes.

- **Exploración de Resultados:** Después de realizar una búsqueda, obtendrás una lista de resultados que coinciden con tus criterios. Cada resultado incluirá detalles como el título del exploit, su ID de CVE (si está disponible), una descripción breve y el enlace para ver más detalles.

- **Detalles del Exploit:** Al hacer clic en un resultado específico, accederás a la página completa del exploit. Aquí encontrarás información detallada sobre la vulnerabilidad, el exploit y cómo funciona. Esto incluye el código del exploit, detalles sobre la vulnerabilidad específica y, a veces, información sobre cómo se puede mitigar o solucionar el problema.

- **Descarga y Uso:** Si tienes experiencia en seguridad informática y estás utilizando Exploit Database con fines legales y éticos, puedes descargar el código del exploit desde la página y usarlo para realizar pruebas de penetración en sistemas o aplicaciones específicas. Sin embargo, es fundamental que utilices Exploit Database de manera responsable y legal, siempre con el permiso adecuado.

[8] Exploit. (s.f.). ExploitDB. [Sitio Web]. Obtenido de Exploit DataBase [consultado el 07 de Octubre 2023]. Disponible en: https://www.exploit-db.com/

- **Contribución:** Si descubres un nuevo exploit o vulnerabilidad, puedes contribuir a Exploit Database enviando la información relevante para que otros puedan beneficiarse de tu investigación.

- **Actualizaciones:** Exploit Database se actualiza regularmente a medida que se descubren y documentan nuevas vulnerabilidades y exploits. Es importante mantenerse al día con las últimas incorporaciones y verificar si hay actualizaciones para las vulnerabilidades que estás investigando.

¿Cómo Articular Con CVE?

Exploit Database (Exploit-DB) y el Glosario de Vulnerabilidades y Exposiciones Comunes (CVE) son dos recursos importantes en el campo de la seguridad cibernética que se utilizan de manera conjunta para identificar, analizar y mitigar vulnerabilidades en sistemas y aplicaciones. A continuación, se explica cómo se pueden articular Exploit-DB y CVE:

- **Búsqueda de CVE en Exploit-DB:** Exploit-DB a menudo proporciona detalles sobre exploits específicos que están relacionados con vulnerabilidades conocidas y documentadas en la base de datos CVE. Puedes buscar exploits en Exploit-DB utilizando términos clave, como el nombre del software o del sistema operativo afectado, y ver si existe un exploit asociado con una vulnerabilidad CVE específica.

- **Relación entre CVE y Exploits:** En la descripción de un exploit en Exploit-DB, es posible que encuentres referencias a un identificador CVE correspondiente a la vulnerabilidad que el exploit aprovecha. Esto ayuda a establecer una relación entre el exploit específico y la vulnerabilidad catalogada en el glosario CVE.

- **Análisis y Validación:** Cuando encuentres un exploit en Exploit-DB que menciona un identificador CVE, puedes utilizar esa información para investigar más a fondo la vulnerabilidad en la base de datos CVE. La entrada de CVE proporcionará detalles adicionales sobre la vulnerabilidad, su gravedad, los sistemas afectados y cualquier parche o solución disponible.

- **Mitigación y Soluciones:** Al identificar una vulnerabilidad en Exploit-DB que está vinculada a un CVE específico, podrás obtener información más completa sobre cómo mitigar o resolver el problema. Puedes encontrar

detalles sobre parches de seguridad, recomendaciones del fabricante y medidas correctivas que ayudarán a proteger los sistemas afectados.

- **Compartir Información:** Si descubres un nuevo exploit o vulnerabilidad que aún no ha sido vinculada a un identificador CVE, puedes contribuir a la comunidad de seguridad informática compartiendo los detalles tanto en Exploit-DB como en la base de datos CVE. Esto ayudará a que otros investigadores y profesionales puedan acceder a la información y tomar las medidas necesarias para proteger sus sistemas.

- **Investigación Avanzada:** La combinación de Exploit-DB y CVE es especialmente valiosa para realizar investigaciones de seguridad más profundas. Puedes utilizar Exploit-DB para acceder a exploits concretos y luego utilizar el identificador CVE para acceder a detalles más técnicos y contextuales en la base de datos CVE.

3 Etapa 2 actuación ética y legal

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

- En cuanto a la definición de protección de datos personales dada por la Ley 1581 de 2012[9], en las consideraciones 1 y 2 además de las cláusulas primera, segunda, tercera, cuarta y quinta dan una mención muy vaga y en ningún momento definen de manera concreta como se van a manejar estos datos. La Ley 1581 de 2012 se refiere a la protección de datos personales y establece requerimientos específicos para el tratamiento de esta información.

[9] publica, D. a. (18 de Octubre de 2012) . [Sitio Web]. Funcion Publica. Obtenido de Ley 1581 de 2012. . [consultado el 07 de Octubre 2023]. Diponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

- Durante todo el documento no se menciona en ninguno de los párrafos acerca del consentimiento informado para la recolección, almacenamiento y tratamiento de los datos, según la Ley 1581, es importante obtener el consentimiento informado de las personas cuyos datos personales se recopilan y procesan.

- En ninguno de los párrafos se hace mención acerca del derecho de los titulares de los datos utilizados. Según lo establecido en la Ley 1581, el derecho de acceso, rectificación, actualización y supresión de la información personal son derechos fundamentales en la protección de datos personales.

- Nunca se menciona cuáles serían las medidas de seguridad tomadas para la transferencia de estos datos fuera del territorio nacional ni de si se informara a los titulares de la información sobre esta transferencia.

- En ninguno de los párrafos detalla cuáles serán las medidas de seguridad técnicas, administrativas y físicas utilizadas para la protección de la información personal, estas medidas están detalladas dentro de la ley 1581.

- La ley exige que las entidades que recolectan y almacenan datos personales registren sus bases de datos en el Registro Nacional de Bases de Datos. No hay mención de esto en ninguno de los párrafos del acuerdo.

- En la Tercera consideración se hace menciona a la protección de la intimidad, la honra y el buen nombre de las personas, pero esta no hace mención en ningún momento como se manejarán estos aspectos de acuerdo con la ley.

- El acuerdo no establece por cuánto tiempo se conservarán los datos confidenciales. La ley establece que los datos personales solo deben conservarse durante el tiempo necesario para cumplir con los fines para los que se recopilaron.

- No se mencionan los derechos y responsabilidades del receptor de los datos confidenciales en relación con la Ley 1581.

- No se contempla en ninguno de los párrafos cómo se manejarán las solicitudes de rectificación y actualización de los datos personales de acuerdo con los derechos de los titulares.

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

Basado en el Anexo 3 y en las fallas identificadas en relación con la Ley 1581[10] de Colombia, estos son los artículos que podrían estar siendo vulnerados:

- **Artículo 2:** Principios de la Ley. El texto no aborda adecuadamente los principios de la ley, como la finalidad, veracidad, seguridad, confidencialidad y otros.

- **Artículo 7:** Consentimiento. No se menciona cómo se obtiene y documenta el consentimiento informado para el tratamiento de datos personales.

- **Artículo 8:** Tratamiento de Datos Sensibles. El texto no distingue ni aborda específicamente el tratamiento de datos sensibles ni su protección adecuada.

- **Artículo 10:** Deberes de los Responsables del Tratamiento. El acuerdo no menciona los deberes y obligaciones del responsable del tratamiento de datos (HackerHouse).
- **Artículo 11:** Deberes de los Encargados del Tratamiento. No se mencionan los deberes y obligaciones de la parte receptora (el estudiante) como encargado del tratamiento de datos.
- **Artículo 12:** Transmisión de Datos a Terceros. No se mencionan las medidas y requisitos para la transmisión de datos a terceros.

- **Artículo 13:** Funciones del Responsable del Tratamiento. El acuerdo no establece cómo se atenderán las solicitudes de los titulares de datos en relación con sus derechos.

- **Artículo 15:** Derechos de los Titulares. No se mencionan los derechos de los titulares de datos personales ni cómo serán ejercidos.

- **Artículo 17:** Registro Nacional de Bases de Datos. No se hace referencia al registro de la base de datos en el Registro Nacional de Bases de Datos.

[10] publica, D. a. (18 de Octubre de 2012) . [Sitio Web]. función Pública. Obtenido de Ley 1581 de 2012. . [consultado el 07 de Octubre 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

- **Artículo 18:** Medidas de Seguridad. El texto no establece cómo se implementarán las medidas de seguridad adecuadas para proteger los datos personales.

- **Artículo 21:** Responsabilidad de los Encargados del Tratamiento. No se abordan las responsabilidades del encargado del tratamiento de datos (la parte receptora) en caso de incumplimientos.

- **Artículo 26:** Transferencia de Datos a Países Extranjeros. No se mencionan las medidas de seguridad y requisitos para las transferencias internacionales de datos.

- **Artículo 27:** Responsabilidad del Responsable y del Encargado del Tratamiento. El texto no aborda adecuadamente la responsabilidad en caso de incumplimientos de los deberes establecidos en la ley.

- **Artículo 28:** Responsabilidad de los Encargados del Tratamiento. No se establece cómo se manejarán los datos confidenciales y las responsabilidades del encargado del tratamiento.

- **Artículo 29:** Excepciones al Consentimiento. El texto no menciona cómo se manejarán las excepciones al consentimiento y el manejo de datos sin consentimiento.

- **Artículo 31:** Derechos del Titular. El acuerdo no establece cómo se manejarán las solicitudes de los titulares de datos en relación con sus derechos.

- **Artículo 37:** Registro Nacional de Bases de Datos. No se hace referencia al registro de la base de datos en el Registro Nacional de Bases de Datos.

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

Rechazaría firmemente el acuerdo propuesto debido a que contraviene numerosos de los principios y deberes fundamentales que todo ingeniero debe acatar, tal como se establece en el Código de Ética[11] que rige nuestra profesión. La infracción de estos principios comprometería la integridad y responsabilidad que los ingenieros tienen en su desempeño.

Un ejemplo claro de estas transgresiones se encuentra en el artículo 34, inciso A del Código de Ética, el cual enfatiza la prohibición categórica de aceptar trabajos que vayan en contra de las disposiciones legales vigentes. Aceptar un acuerdo que no cumple con los estándares éticos y legales establecidos equivaldría a una clara violación de este precepto, socavando la credibilidad y el compromiso con el cumplimiento de la ley que debe prevalecer en la actuación de un ingeniero.
Asimismo, el artículo 35, inciso b, establece la imperiosa obligación de respetar y asegurar el respeto de todas las disposiciones legales y reglamentarias en el ejercicio de la profesión. Esto implica no solo el respeto personal, sino también el deber de denunciar cualquier violación o irregularidad que se detecte. Aceptar un acuerdo que no cumple con los estándares éticos y legales implicaría no solo la falta de respeto por la ley, sino también la omisión en el deber de denunciar posibles transgresiones.

El inciso C del mismo artículo enfatiza la responsabilidad de velar por el prestigio de la profesión. Un acuerdo que no se ajusta a los principios éticos y legales puede poner en riesgo la imagen y la confianza en los ingenieros como profesionales responsables y comprometidos. Además, el Código de Ética establece la obligación de denunciar cualquier infracción o falta al código que el ingeniero tenga conocimiento en el ejercicio de su profesión. No cumplir con este deber de denuncia puede resultar en la propagación de conductas incorrectas y en la perpetuación de comportamientos inadecuados en el ámbito profesional.
Por último, el código establece el deber de custodiar y proteger los bienes, valores, documentos e información confiados al ingeniero. Al no asegurarse de que los datos confidenciales y la información se manejen de manera adecuada y segura, estaríamos incumpliendo con nuestra responsabilidad de custodiar los recursos encomendados y garantizar su correcto uso.

En conclusión, la aceptación de un acuerdo que no cumple con los principios éticos y legales establecidos en nuestro Código de Ética equivaldría a traicionar nuestra profesión y nuestra responsabilidad con la sociedad. Es fundamental que como ingenieros nos mantengamos fieles a los principios y deberes que establece COPNIA, salvaguardando la confianza y la integridad que se espera de nosotros en cada paso de nuestra labor profesional.

[11] COPNIA. (2015). [Sitio Web]. Código de ética. Obtenido de Consejo Profesional Nacional de Ingenieria [consultado el 15 de Agosto 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

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

El articulo consultado se titula ¡Cuidado! Delincuentes están usando códigos QR para estafar a sus víctimas[12] donde se advierte sobre el uso de códigos QR por parte de delincuentes para cometer estafas. Se señala cómo estos códigos QR están siendo utilizados en diversos engaños, como redireccionar a sitios web falsos o robar información personal y bancaria de las víctimas. Se destaca la importancia de verificar la autenticidad de los códigos QR antes de escanearlos y se ofrecen recomendaciones para prevenir ser víctima de estas estafas. Además, se mencionan casos concretos de personas que han sido afectadas por esta modalidad de fraude.

La proliferación de estafas utilizando códigos QR es una muestra de cómo los delincuentes están adaptándose a la tecnología para aprovecharse de la confianza y la conveniencia que estos códigos ofrecen. Es crucial que los usuarios se mantengan alerta y sigan prácticas de seguridad sólidas al interactuar con códigos QR, como verificar su autenticidad antes de escanearlos y evitar proporcionar información personal sensible a través de estos códigos.

Esta situación también subraya la importancia de la educación en seguridad cibernética para el público en general. Los usuarios deben ser conscientes de las posibles amenazas en línea y estar equipados con el conocimiento necesario para protegerse a sí mismos. A medida que la tecnología evoluciona, es fundamental mantenerse informado sobre las tácticas de estafa en constante cambio y tomar medidas proactivas para protegerse contra ellas.
En última instancia, aunque la conveniencia de los códigos QR es innegable, esta noticia nos recuerda que siempre debemos ser cautelosos y diligentes al interactuar con la tecnología, especialmente cuando se trata de compartir información personal o financiera.

Los posibles artículos de la Ley 1273[13] que podrían estar involucrados en casos de estafas con códigos QR son:

---

[12] Espectador, R. T. (21 de Enero de 2022). [Sitio Web]. ¡Cuidado! Delincuentes están usando códigos QR para estafar a sus víctimas. Obtenido de EL ESPECTADOR [consultado el 15 de Agosto 2023]. Disponible en: https://www.elespectador.com/tecnologia/cuidado-delincuentes-estan-usando-codigos-qr-para-estafar-a-sus-victimas/

[13] Colombia, R. d. (5 de Enero de 2009). [Sitio Web]. SIC. Obtenido de LEY 1273 DE 2009 [consultado el 07 de Octubre 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

- **Artículo 269C. Interceptación De Datos Informáticos**: Este artículo establece que el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, incidirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269F. Violación de datos personales**: Este artículo establece que quien, sin autorización y en perjuicio de otro, acceda, capture, intercepte, modifique, suprima, destruya o divulgue información contenida en un sistema informático, incidirá en penas que pueden ir desde prisión hasta una multa.

- **Artículo 269G. Suplantación De Sitios Web Para Capturar Datos Personales:** Este artículo establece que quien con intenciones ilícitas y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, y puede incurrir en ´pena de prisión, una multa siempre que no incurra en delitos más graves.

- **Artículo 2691. Hurto Por Medios Informáticos Y Semejantes**: Este artículo establece que la persona que, manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incidirá en las penas señaladas en el artículo 240 de este Código.

En todos los casos, si alguien utiliza códigos QR para redirigir a sitios web falsos o robar información personal y bancaria, podrían estar infringiendo estos artículos. Las consecuencias legales podrían incluir penas de prisión y multas, cuya duración y monto dependerán de la gravedad de la infracción y de las circunstancias específicas de cada caso.

4 Etapa 3 ejecución pruebas de intrusión

Objetivos del Ejercicio

El ejercicio de Red Team tiene los siguientes objetivos clave:

- ✓ Evaluar la resistencia de las defensas de seguridad de la Empresa HackerHouse contra amenazas cibernéticas realistas y ataques avanzados.
- ✓ Identificar y documentar debilidades en la infraestructura, aplicaciones, políticas y procedimientos de seguridad.
- ✓ Evaluar la capacidad de respuesta del equipo de seguridad de la Empresa HackerHouse ante incidentes de seguridad.

- ✓ Proporcionar recomendaciones concretas y acciones correctivas para mejorar la seguridad y la preparación para amenazas cibernéticas.

Alcance del Ejercicio

El alcance del ejercicio de Red Team incluirá lo siguiente:

- ✓ Evaluación del equipo de cómputo que contiene un Windows 10 X64.
- ✓ Evaluación de la seguridad de las aplicaciones web y móviles en uso por la empresa.
- ✓ Pruebas de ingeniería social limitadas para evaluar la conciencia de seguridad del personal y la respuesta ante correos electrónicos.

Metodología Utilizada

Para llevar a cabo este ejercicio de Red Team, se utilizará una metodología integral que incluirá las siguientes fases:

- **Reconocimiento y Recopilación de Información:** Se recopilará información sobre la empresa y sus activos, principalmente sobre el equipo de cómputo comprometido.

- **Escaneo y Enumeración:** Se llevará a cabo un escaneo de red para identificar servicios y sistemas disponibles. Se realizará una enumeración de servicios y aplicaciones para obtener información adicional.

- **Exploración de Vulnerabilidades:** Se identificarán posibles vulnerabilidades en sistemas y aplicaciones y se evaluará su explotabilidad.

- **Pruebas de Penetración:** Se realizarán pruebas de penetración éticas para explotar vulnerabilidades y ganar acceso a sistemas o datos sensibles.

- **Escalada de Privilegios**: Se buscarán oportunidades para escalar privilegios y obtener un mayor control sobre los sistemas comprometidos.

- **Mantenimiento de Acceso:** Se evaluarán técnicas para mantener el acceso a sistemas comprometidos incluso después de reinicios.

- **Documentación y Presentación de Informes:** Se documentarán detalladamente todas las actividades, hallazgos y recomendaciones, y se presentarán en un informe completo.

Descripción de la Infraestructura y Sistemas Objetivo

La organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos:

Nombre_estudiante_codigo_fecha_actividad, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

- Tenía un S.O Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante

Resumen Ejecutivo

Ejercicio de Red Team - Empresa HackerHouse

Fecha: 10 septiembre de 2023

Equipo de Red Team: Mishell Karina Rojas Montealegre

Hallazgos Clave:

Durante el ejercicio de Red Team llevado a cabo en la infraestructura de la Empresa HackerHouse, se identificaron una serie de hallazgos críticos y preocupantes que requieren atención inmediata. Los principales hallazgos son los siguientes:

- **Vulnerabilidad de DLL Hijacking**: Se detectó una vulnerabilidad crítica de escalda de privilegios utilizando la vulnerabilidad CVE-2019-0841 para obtener control de archivos para ejecutar código malicioso y secuestrar dichos archivos.

- **Falta de Parches Críticos**: Se identificaron sistemas que no han recibido parches de seguridad críticos. Esto deja la infraestructura vulnerable a ataques conocidos que podrían resultar en la explotación exitosa.

- **Vulnerabilidad de Escalada de Privilegios:** Se identifico una vulnerabilidad critica por la cual utilizando bypass para eludir el control de acceso mediante el archivo fodhelper.exe para acceder a una consola en modo administrador.

- **Acceso Remoto a la Maquina:** Se detecto un acceso ilegal a la maquina mediante un túnel por el puerto 443 por la ejecución de código malicioso.

Recomendaciones Clave:

Para mitigar los riesgos identificados y fortalecer la seguridad de la infraestructura, se recomiendan las siguientes acciones inmediatas:

- **Aplicación de Parches Críticos:** Se debe priorizar la aplicación de los parches de seguridad críticos en todos los sistemas y servidores afectados.

- **Evitar Descargas de Software Desconocido:** Se deben implementar políticas para evitar descargas ilegales o descargas de archivos o ejecutables de origen desconocido.

- **Auditoría de Seguridad Continua:** Se recomienda implementar una auditoría de seguridad continua para detectar y mitigar amenazas de manera proactiva.

- **Formación en Seguridad:** Se debe proporcionar capacitación en seguridad cibernética a todo el personal para aumentar la conciencia y la capacidad de respuesta ante amenazas.

- **Monitorización de Eventos de Seguridad:** Se debe establecer una monitorización continua de eventos de seguridad para detectar actividad inusual o sospechosa y responder de manera eficaz.

- **Cierre de Puerto:** Se debe realizar un cierre de puertos TCP que no se encuentren utilizando para evitar accesos no autorizados.

Estas recomendaciones son cruciales para garantizar la seguridad de la Empresa HackerHouse y reducir la exposición a posibles amenazas. Se insta a la dirección y al equipo de seguridad a tomar medidas inmediatas para abordar los hallazgos y fortalecer la postura de seguridad de la organización.

Detalles Técnicos

Hallazgo 1: Vulnerabilidad de Acceso Remoto a la Maquina

Descripción: El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: Mishell_Karina_Rojas_1010142031_10092023, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente. El administrador de la computadora afectada menciona que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

Pruebas Realizadas: primero se realizó un escaneo de puertos a la red de la compañía para identificar posibles puertos extraños que se encuentren abiertos, para esto se utilizó la herramienta nmap para hacer un escaneo de la red (*Ilustración* 1).

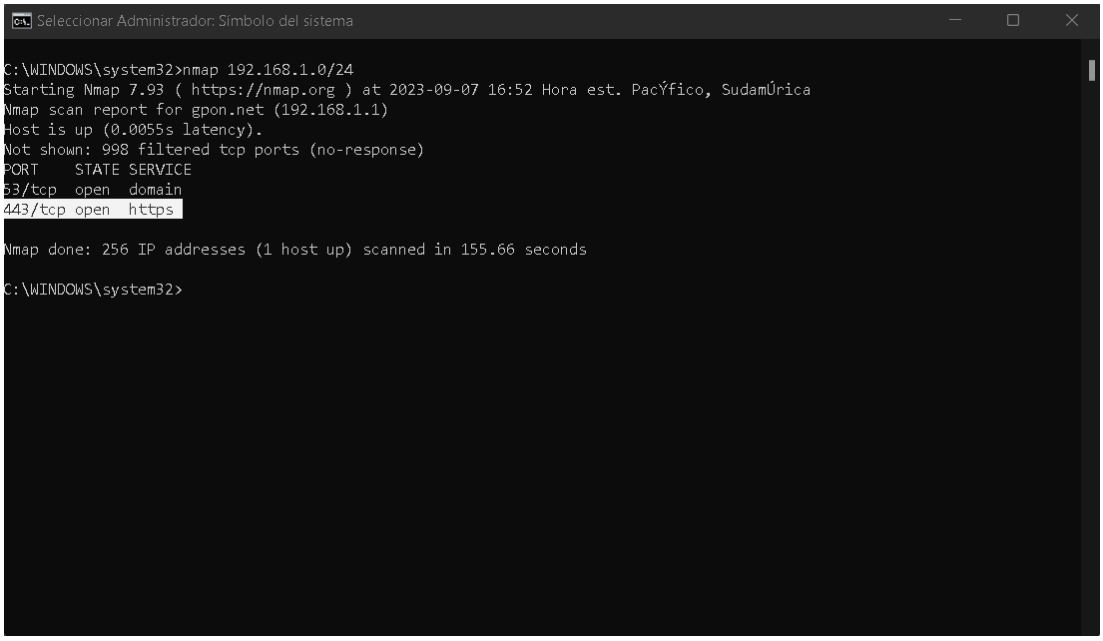

Ilustración 1. Escaneo de puertos en la red

Fuente: Creación propia del estudiante

Luego se procede con la simulación de la vulnerabilidad para esto se realizó un payload que realice la conexión mediante el puerto identificado a una maquina atacante, esto se realizó utilizando el programa msfvenom (*Ilustración* 2)

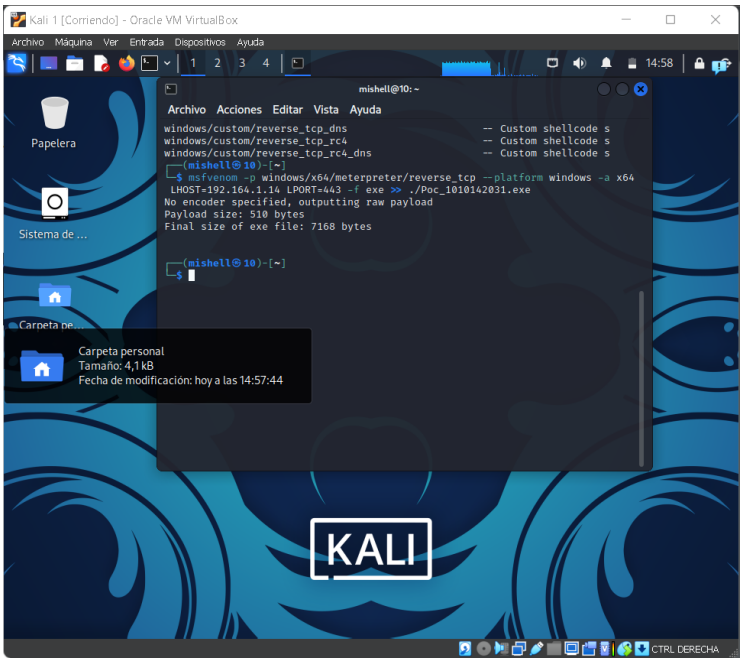

Ilustración 2. Creación del payload

Fuente: Creación propia del estudiante

Luego de crear este payload se procede a enviar el ejecutable a la maquina víctima, para la ejecución del archivo se utilizó ingeniería social escondiendo el ejecutable dentro de un software que parecía inofensivo y convenciendo al usuario que este archivo es inofensivo. (*Ilustración* 3)

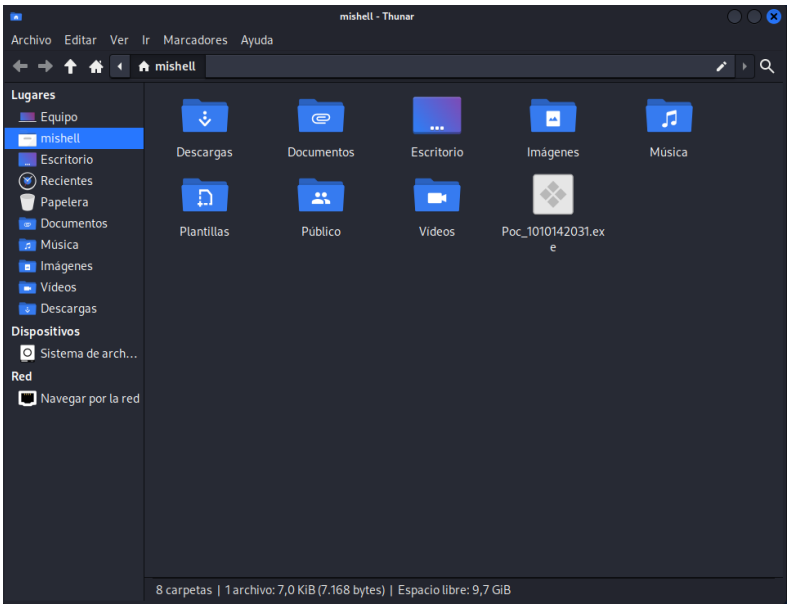

Ilustración 3. Payload Ejecutable

Fuente: Creación propia del estudiante

Y por último se utiliza el software meta exploit framework configurándolo con los datos de la ip, el puerto de escucha y el exploit para realizar la conexión con la maquina víctima. Para esto se utilizó el exploit Windows/x64/meterpreter/reverse_tcp. (*Ilustración* 4)

Ilustración 4. Configuración del metaexploit

Fuente: Creación propia del estudiante

Por último, se realizó la ejecución del exploit para esperar que se conecte un cliente y con esto logramos acceder mediante consola meterpreter a la maquina víctima. (*Ilustración* 5)

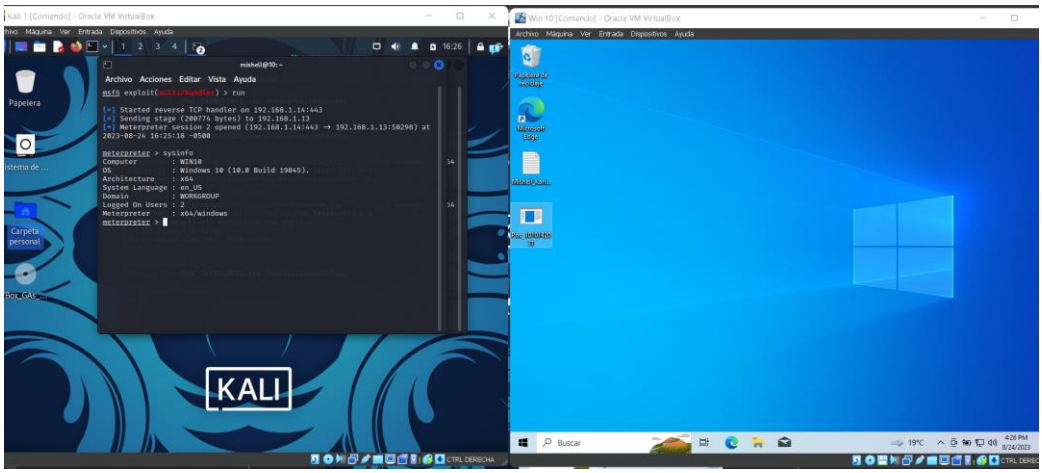

Ilustración 5. Conexión Meterpreter

Fuente: Creación propia del estudiante

Las pruebas de explotación tuvieron éxito, lo que demostró la existencia de una vulnerabilidad de acceso remoto no autorizado que es una vulnerabilidad crítica. Se obtuvo acceso a la consola cmd de la maquina win 10, además de poder utilizar ciertas herramientas de espía como acceso a la cámara, acceso a screenshots sin autorización del usuario, keygen para detección de teclado y ejecución de comandos de manera remota.

Hallazgo 2: Escalada De Privilegios Con CVE-2019-0841.
Para iniciar este proceso se utiliza la conexión existente con meterpreter para acceder a la consola cmd de Windows y tener la información de la máquina. (*Ilustración* 6)

Ilustración 6. Información de la maquina victima

Fuente: Creación propia del estudiante

Luego de esto se guarda un archivo con la información de la maquina y utilizando el comando Download se descarga el archivo desde la maquina víctima. (*Ilustración 7*)

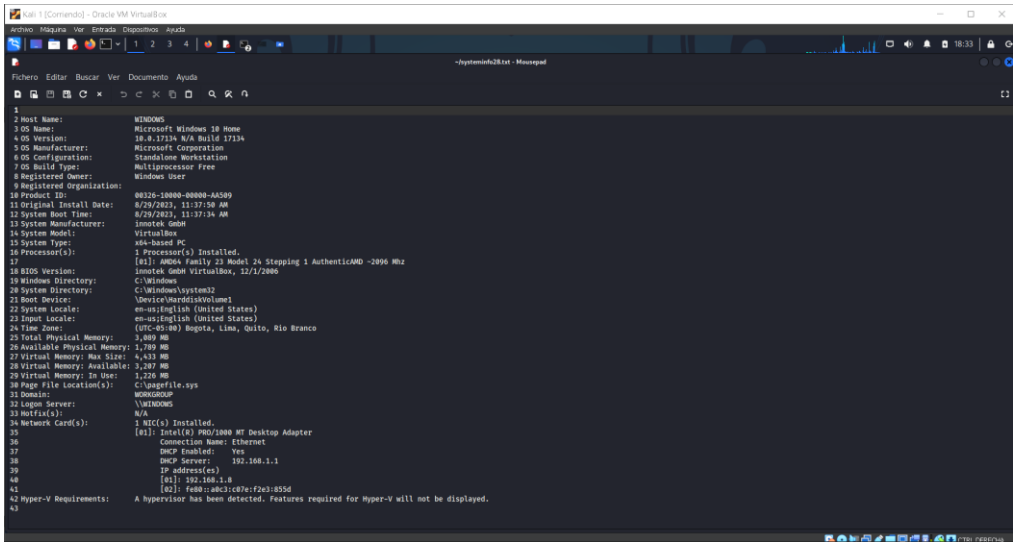

Ilustración 7. Archivos con la información de la maquina victima en KALI

Fuente: Creación propia del estudiante

Ya con los datos completos de la maquina víctima se descarga el programa wesng, utilizando el comando python wes.py win10_exploits.txt, el cual se encarga de tomar todos los datos de la maquina Windows y detectar las vulnerabilidades existentes y los parches que tenga instalados la máquina. (*Ilustración 8*)

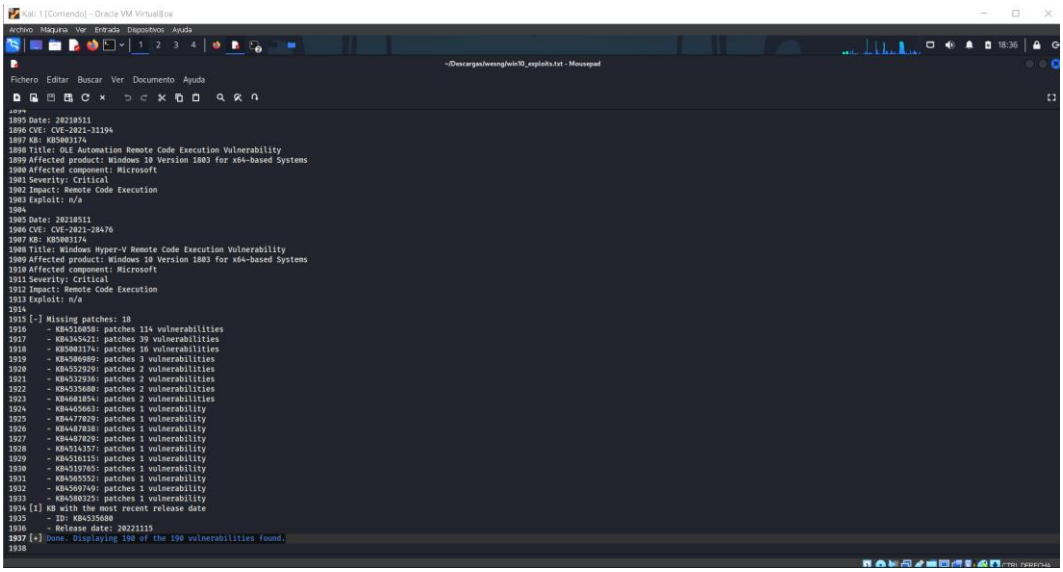

Ilustración 8. Archivo con todas las vulnerabilidades de Windows

Fuente: Creación propia del estudiante

Ya habiendo identificado que la vulnerabilidad existe dentro de la máquina, se procede a descargar el ejecutable WindowsAppsLPE.exe el cual es el encargado de secuestrar archivos que son propiedad de NTAuthority\SYSTEM. Esto se realiza sobrescribiendo los permisos en el archivo destino, el que se quiere secuestrar. (*Ilustración* 9)

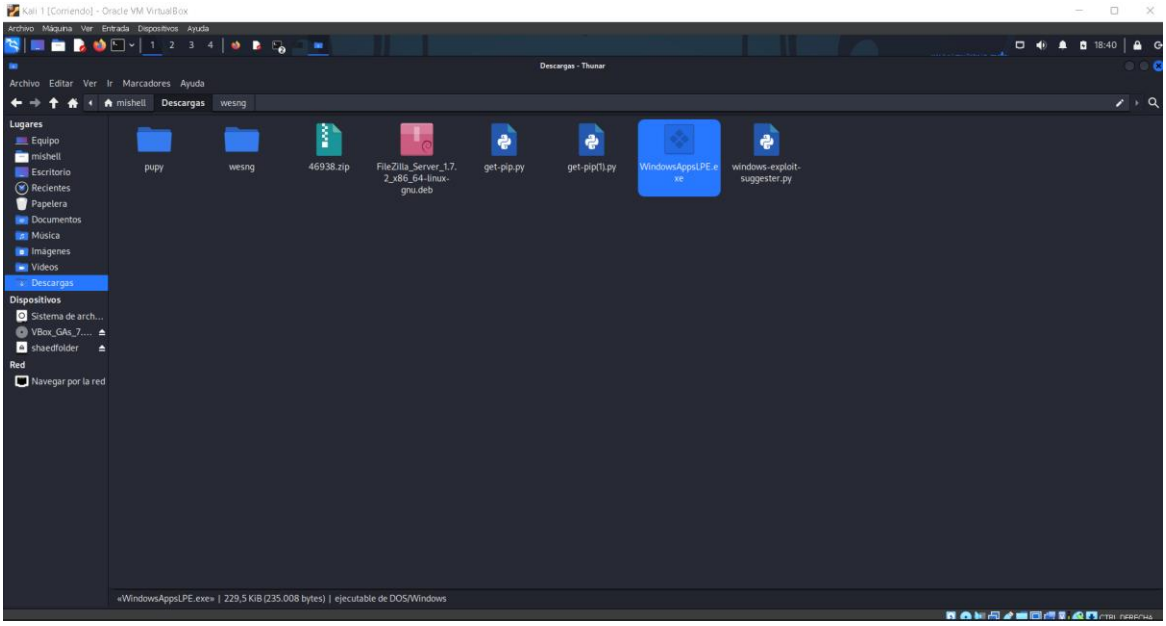

Ilustración 9. Archivo ejecutable WindowsAppsLPE.exe

Fuente: Creación propia del estudiante

Luego se utiliza el comando upload dentro de la consola meterpreter para enviar el archivo a la maquina victima para poder realizar la escalada de privilegios. Para este ejercicio se realiza le escalada sobre el archivo de hosts para darle permisos totales al usuario Mishell el cual no posee privilegios elevados. (*Ilustración* 10)

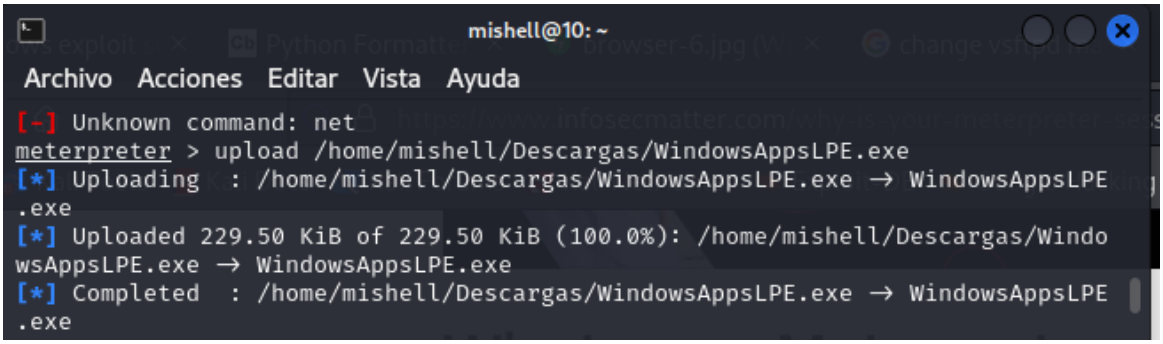

Ilustración 10. Cargue del archivo a la maquina victima Windows

Fuente: Creación propia del estudiante

Por último se ejecuta desde meterpreter los comandos necesarios para realizar la escalada de permisos sobre el archivo de hosts en la maquina víctima y tener el control total de este documento. (*Ilustración 11*).

Ilustración 11. Secuestro del archivo hosts

Fuente: Creación propia del estudiante

Las pruebas de explotación tuvieron éxito, lo que demostró la existencia de una vulnerabilidad de escalda de permisos y ejecución de código remoto. Como observamos el archivo hosts ahora posee todos los permisos sobre el usuario Mishell. (*Ilustración 12*).

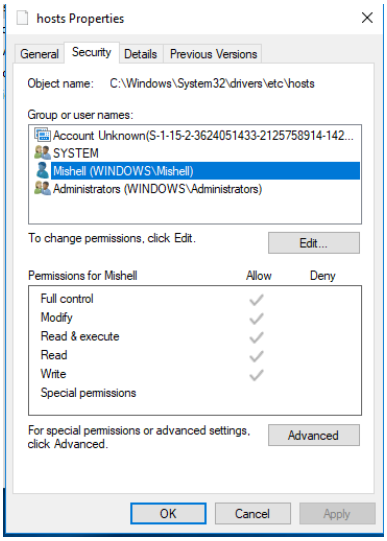

Ilustración 12. Propiedades del archivo hosts con todos los permisos

Fuente: Creación propia del estudiante

Hallazgo 3: Escalada de Privilegios.

Para este proceso de obtener el control del usuario de administrador en la maquina victima debemos primero tener una sesión activa de meterpreter. Luego de tener esta sesión debemos utilizar el exploit explot/Windows/local/bypassuac_fodhelper el cual nos ayudara a realizar el proceso de bypass a la máquina. (*Ilustración 13*).

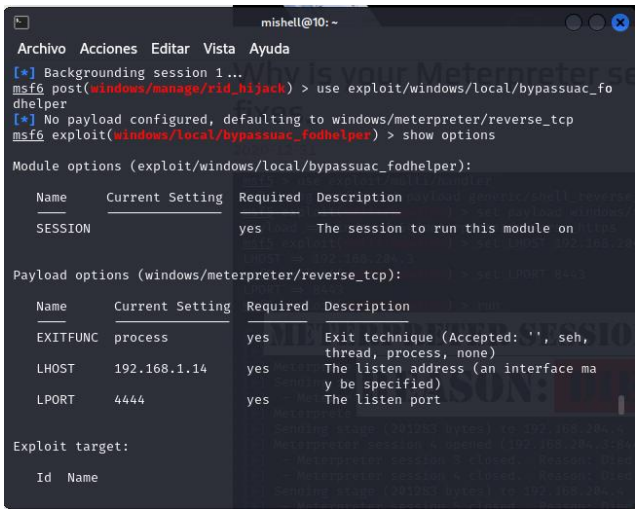

Ilustración 13. Configuración del exploit bypass

Fuente: Creación propia del estudiante

Luego de configurar el exploit de bypass y configurar todos los datos de la conexión meterpreter, lo más importante para este caso es haber enviado a segundo plano la sesión de meterpreter con el comando background y obtener su id de sesión con el comando sessions. Por último ejecutamos el exploit con el comando run. (*Ilustración 14*).

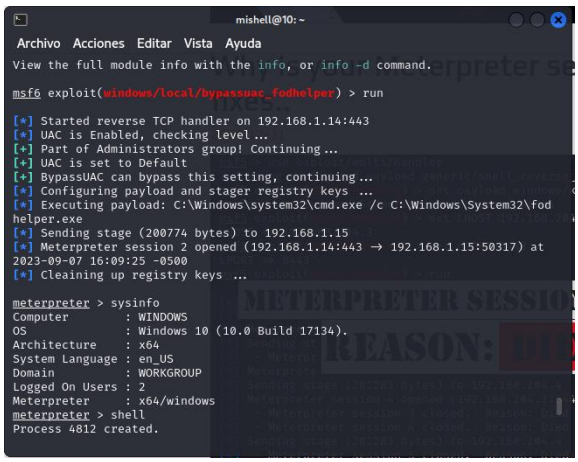

Ilustración 14. Ejecución del bypass y sesión del administrador

Fuente: Creación propia del estudiante

Por último habiendo obtenido acceso mediante administrador procedemos a crear un usuario nuevo para poder realizar todas las acciones necesarias mediante ese usuario de manera incognita. (*Ilustración 15*).

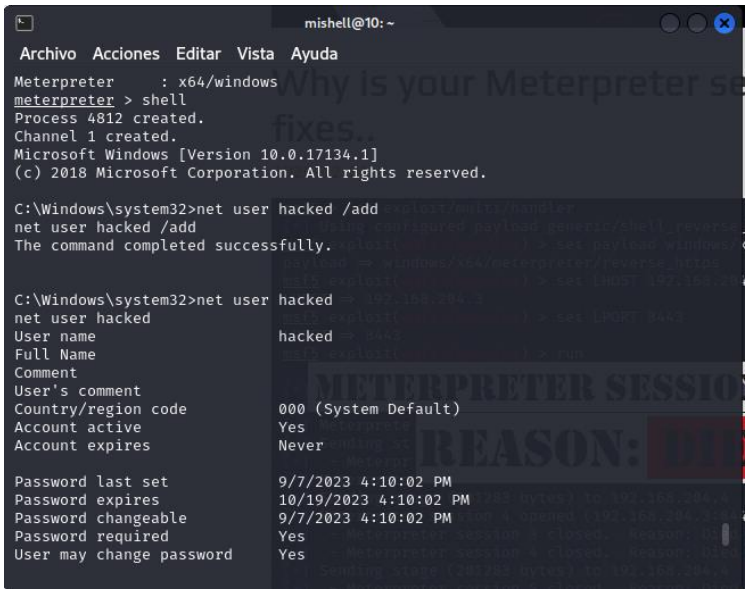

Ilustración 15. Creación de un usuario

Fuente: Creación propia del estudiante

Por último se le da un permiso de administrador al usuario que creamos para lograr realizar acciones sobre la maquina victima sin necesitar ningún permiso adicional. (*Ilustración* 16).

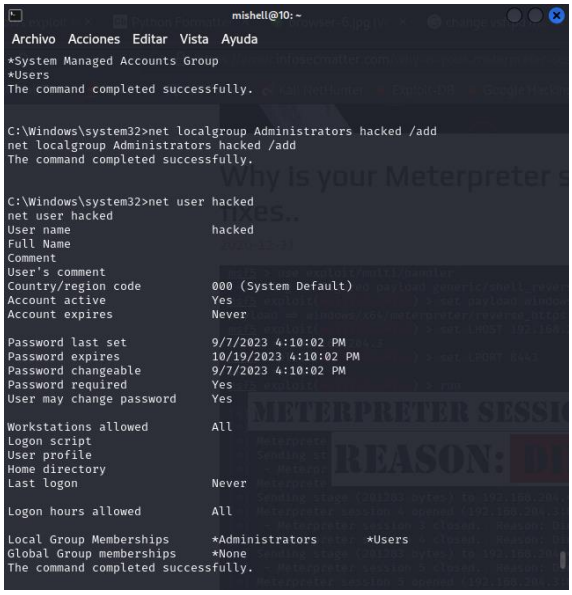

Ilustración 16. agregar permisos de administrador al usuario creado

Fuente: Creación propia del estudiante

Las pruebas de explotación tuvieron éxito, lo que demostró la existencia de una vulnerabilidad de escalda de permisos y ejecución de código remoto. Como observamos ahora dentro del sistema Windows 10 podemos ver un usuario llamado hacked el cual fue creado de manera ilegal y remotamente mediante la consola de meterpreter. (*Ilustración* 17).

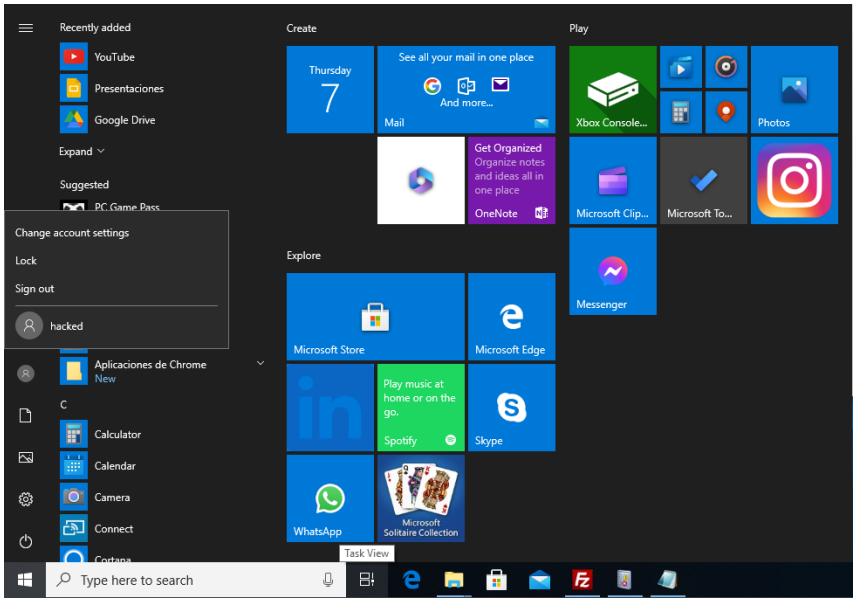

Ilustración 17. Usuario Hacked creado

Fuente: Creación propia del estudiante

Impacto Potencial de los Hallazgos

Escalada de Privilegios: Se identificó una vulnerabilidad de escalada de privilegios en un equipo Windows 10 de uno de los colaboradores. Esta vulnerabilidad representaba un riesgo crítico, ya que permitía a un atacante obtener acceso de administrador al sistema comprometido.

Hijacking de Archivos: Se descubrió una debilidad en la seguridad de los sistemas de archivos que podría permitir a un atacante tomar el control de archivos críticos en la maquina corporativa. Esta amenaza potencial plantea preocupaciones de confidencialidad e integridad de los datos.

Acceso Remoto mediante Meterpreter: A través de técnicas de explotación avanzadas, se logró obtener acceso remoto a sistemas críticos utilizando Meterpreter, una herramienta de código abierto de Metasploit. Esto puso de manifiesto la importancia de la detección y la respuesta eficaz a incidentes.

Evaluación de las Repercusiones en la Organización
La Empresa HackerHouse debe considerar cuidadosamente las posibles repercusiones de los hallazgos identificados durante el ejercicio de Red Team:

- **Pérdida de Datos Sensibles:** La vulnerabilidad de escalada de privilegios y las contraseñas débiles pueden dar lugar a la pérdida de datos sensibles o confidenciales de la empresa y sus clientes, lo que podría tener un impacto negativo en la confianza y la conformidad con las regulaciones.

- **Interrupción de Servicios:** Un ataque exitoso basado en los hallazgos podría resultar en la interrupción de servicios críticos, lo que afectaría la operación normal de la empresa y posiblemente causaría pérdidas financieras.

- **Daño a la Reputación:** La divulgación de una brecha de seguridad o de un incidente cibernético puede dañar la reputación de la Empresa HackerHouse y socavar la confianza de los clientes, socios y partes interesadas.

- **Repercusiones Legales y Regulatorias:** Dependiendo de la naturaleza de los hallazgos, la empresa podría enfrentar consecuencias legales y regulatorias, incluyendo multas y sanciones.

Recomendaciones

Con base en los hallazgos del ejercicio de Red Team, se presentan las siguientes medidas específicas para mitigar los riesgos identificados:

- **Aplicación de Parches y Actualizaciones de Seguridad**: Se recomienda aplicar los parches y actualizaciones de seguridad más recientes para el servidor de aplicaciones. Esto abordará la vulnerabilidad de escalada de privilegios identificada.

- **Auditorías de Seguridad Continuas:** Implementar auditorías de seguridad regulares para detectar y mitigar posibles vulnerabilidades de forma proactiva.

- **Educar al Personal**: Proporcionar capacitación en seguridad cibernética a todo el personal para aumentar la conciencia sobre la importancia de contraseñas seguras y prácticas de autenticación.

- **Gestión de Parches:** Implementar un proceso de gestión de parches eficaz que asegure la aplicación oportuna de parches de seguridad críticos en todos los sistemas.
- **Monitorización de Eventos de Seguridad:** Establecer una monitorización continua de eventos de seguridad para detectar actividad inusual o posibles amenazas después de aplicar los parches.

Recomendaciones Generales para Mejorar la Seguridad y Robustez del Sistema

Además de las medidas específicas para abordar los hallazgos, se recomiendan las siguientes prácticas generales para mejorar la seguridad y robustez del sistema:

- **Evaluación Regular de la Infraestructura:** Realizar evaluaciones regulares de seguridad de la infraestructura y las aplicaciones para identificar y abordar nuevas vulnerabilidades.

- **Políticas y Procedimientos de Seguridad Actualizados:** Mantener y actualizar políticas y procedimientos de seguridad cibernética para reflejar las mejores prácticas y las amenazas emergentes.

- **Ejercicios de Concienciación en Seguridad:** Realizar ejercicios regulares de concienciación en seguridad para todo el personal para fomentar buenas prácticas de seguridad.

- **Respuesta a Incidentes**: Desarrollar y mantener un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad.

- **Auditorías Externas:** Considerar auditorías de seguridad externas periódicas para obtener una evaluación independiente de la seguridad.

- **Seguimiento de Cumplimiento: Asegurar** el cumplimiento de regulaciones y estándares de seguridad relevantes, como GDPR, HIPAA, ISO 27001, etc.

5 Etapa 4 contención de ataques informáticos

- ✓ **¿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.**

Como un experto en ciberseguridad se deben seguir una serie de pasos para identificar y responder adecuadamente a la amenaza. Estos pasos pueden variar según la naturaleza del ataque, pero aquí hay una lista general de pasos a seguir, los cuales son:

- o **Detección de Anomalías**

La detección de anomalías es una parte fundamental de la ciberseguridad, ya que permite identificar patrones inusuales o comportamientos anómalos en una red o sistema que pueden indicar un posible ataque. Sin embargo, es importante recordar que ningún sistema de detección es infalible, y es fundamental contar con una estrategia de seguridad en capas que incluya medidas preventivas y procedimientos de respuesta a incidentes para proteger adecuadamente una organización contra las amenazas cibernéticas. La detección de anomalías puede incluir:

- **Sistemas de Detección de Intrusiones (IDS) e Intrusion Prevention Systems (IPS):** Los IDS y los IPS son herramientas que supervisan constantemente el tráfico de red en busca de comportamientos sospechosos. Los IDS detectan intrusiones y emiten alertas, mientras que los IPS pueden tomar medidas para bloquear automáticamente actividades maliciosas. Estos sistemas se basan en firmas conocidas y reglas predefinidas para identificar actividades maliciosas o patrones de tráfico anómalos.

- **Machine Learning y Análisis de Comportamiento:** Además de las reglas predefinidas, muchas soluciones modernas utilizan técnicas de aprendizaje automático y análisis de comportamiento para identificar anomalías. Esto implica la creación de modelos de comportamiento normales y la identificación de desviaciones significativas de estos modelos. Por ejemplo, si un usuario que normalmente solo accede a ciertas carpetas comienza a acceder a archivos sensibles, esto podría ser considerado una anomalía.

- **Análisis de Registros y Eventos:** La revisión de registros y eventos de seguridad es crucial. Los registros contienen información detallada sobre lo que sucede en una red o sistema. Los expertos en seguridad analizan estos registros en busca de patrones inusuales, como intentos de acceso fallidos,

cambios de configuración inesperados o actividad de usuarios que no coincide con los patrones típicos.

- **Alertas y Priorización:** Cuando se detecta una anomalía, se genera una alerta. Estas alertas pueden variar en gravedad, y el equipo de seguridad debe priorizarlas en función de la amenaza percibida. No todas las anomalías son igualmente importantes, por lo que se debe enfocar la atención en las que representan un riesgo significativo.

- **Correlación de Eventos:** A menudo, se deben correlacionar múltiples eventos y alertas para obtener una imagen completa de lo que está ocurriendo. Por ejemplo, una sola alerta de intento de inicio de sesión fallido podría no ser preocupante, pero si se correlaciona con otros eventos sospechosos, podría indicar un intento de intrusión más amplio.

- **Umbral de Falsos Positivos:** La detección de anomalías puede generar falsos positivos, es decir, alertas que parecen indicar un ataque pero que son inofensivas. Es importante ajustar los umbrales y las reglas para reducir la cantidad de falsos positivos y centrarse en las amenazas reales.

- **Alertas de Seguridad**

Las alertas de seguridad son notificaciones generadas por herramientas y sistemas de seguridad que indican la detección de actividades o eventos que podrían ser indicativos de una amenaza o un ataque cibernético. Estas alertas desencadenan la respuesta del equipo de seguridad de la organización. Un proceso efectivo de gestión de alertas permite a una organización identificar y responder a las amenazas de manera oportuna, minimizando el impacto potencial de los ataques y protegiendo la integridad y la disponibilidad de los sistemas y datos críticos.

- **Recopilación de Información**

La "Recopilación de Información" es un paso crucial en la respuesta a un ataque informático en tiempo real, ya que implica la recopilación de datos relevantes sobre la actividad sospechosa o el incidente de seguridad. La recopilación de información es un paso crítico para comprender la naturaleza y el alcance del incidente de seguridad, identificar a los actores involucrados y tomar las medidas necesarias para mitigar el impacto. La información recopilada se utilizará en investigaciones posteriores, informes de incidentes y acciones de respuesta.

- **Análisis de Tráfico**

El "Análisis de Tráfico" es un componente importante en la respuesta a un ataque informático en tiempo real, ya que permite comprender cómo se está llevando a

cabo el ataque, qué sistemas o servicios se están viendo afectados y cómo se pueden tomar medidas para mitigar la amenaza. El análisis de tráfico es una habilidad crítica en la respuesta a incidentes de seguridad, ya que proporciona información clave para la comprensión y la mitigación de amenazas. La capacidad de identificar patrones y comportamientos anómalos en el tráfico de red es esencial para una respuesta efectiva a incidentes cibernéticos.

- **Recolección de Evidencia**

La "Recolección de Evidencia" es un paso fundamental en la respuesta a un ataque informático en tiempo real. Esta fase implica la preservación de cualquier tipo de evidencia digital relacionada con el incidente para fines de investigación, análisis forense y, en algunos casos, posibles acciones legales. La recolección de evidencia es esencial para determinar la causa y el alcance de un incidente de seguridad y para tomar las medidas apropiadas para mitigar los riesgos y prevenir futuros incidentes. Es importante que esta fase se realice de manera cuidadosa y profesional para garantizar la integridad y la confiabilidad de la evidencia.

- **Determinación de la Fuente**

La "Determinación de la Fuente" es un paso crítico en la respuesta a un ataque informático en tiempo real, ya que implica la identificación de la fuente o el origen del ataque. La determinación de la fuente de un ataque puede ser un proceso complejo y, en algunos casos, puede ser difícil de lograr, especialmente si los atacantes han tomado medidas para ocultar su identidad. Sin embargo, es un paso esencial para tomar medidas legales o técnicas adicionales para mitigar el riesgo y proteger la infraestructura de la organización.

- **Notificación de Incidentes**

La "Notificación de Incidentes" es un paso crítico en la respuesta a un ataque informático en tiempo real, ya que implica informar a las partes interesadas y a las autoridades pertinentes sobre el incidente de seguridad. La notificación de incidentes es esencial para una respuesta efectiva, ya que permite una acción rápida y coordinada para abordar la amenaza y minimizar el impacto en la organización. Además, el cumplimiento de los requisitos legales y regulatorios de notificación es fundamental para evitar posibles sanciones y pérdida de confianza de los clientes y socios comerciales.

- **Mitigación y Contención**

La "Mitigación y Contención" es un paso crítico en la respuesta a un ataque informático en tiempo real, ya que tiene como objetivo detener la actividad maliciosa, minimizar el impacto del incidente y proteger los sistemas y datos de la organización. La mitigación y contención son esenciales para limitar el alcance y el

impacto de un incidente de seguridad. Un enfoque rápido y coordinado para detener la actividad maliciosa y proteger los activos de la organización es fundamental para minimizar el daño y restaurar la seguridad de los sistemas y datos.

- **Recuperación y Restauración**

La "Recuperación y Restauración" son fases críticas en la respuesta a un ataque informático, ya que implican la restauración de sistemas y datos afectados a un estado funcional normal después de un incidente. La recuperación y la restauración son esenciales para restablecer la normalidad después de un incidente de seguridad. La rapidez y la eficacia en la recuperación y restauración son fundamentales para minimizar el tiempo de inactividad y el impacto en la organización, así como para restaurar la confianza de los clientes y socios comerciales.

La recuperación puede incluir los siguientes pasos:

- **Evaluación de Daños:** Antes de iniciar la recuperación, es importante evaluar los daños causados por el incidente. Esto incluye determinar qué sistemas, datos y recursos se vieron afectados y en qué medida.

- **Priorización de la Recuperación:** En función de la evaluación de daños, prioriza la recuperación de sistemas y datos. Identifica qué sistemas y datos son críticos para la operación continua de la organización y dales prioridad en el proceso de recuperación.

- **Restauración de Sistemas y Datos:** Utiliza copias de seguridad (si están disponibles y no se vieron comprometidas) o sistemas limpios para restaurar los sistemas afectados a un estado funcional normal. Asegúrate de que los sistemas restaurados estén debidamente parcheados y actualizados para prevenir futuras vulnerabilidades.

- **Pruebas de Recuperación:** Después de la restauración, realiza pruebas exhaustivas para garantizar que los sistemas funcionen como se espera. Esto incluye pruebas de funcionalidad, rendimiento y seguridad.

- **Restablecimiento de Credenciales:** Si se han visto comprometidas credenciales de usuario o contraseñas, asegúrate de restablecerlas y comunicar los cambios a los usuarios afectados.

- **Monitoreo Continuo:** Una vez que los sistemas se han recuperado, continúa monitoreándolos de cerca en busca de signos de actividad maliciosa o problemas persistentes.

La restauración puede incluir los siguientes pasos:

- **Evaluación de Integridad de Datos:** Verifica la integridad de los datos restaurados para asegurarte de que no se hayan corrompido durante el incidente o la recuperación. Esto es especialmente importante si se ha visto afectado el almacenamiento de datos críticos.

- **Restauración de Configuraciones:** Asegúrate de que las configuraciones de los sistemas, aplicaciones y servicios se restablezcan correctamente a sus estados anteriores y cumplan con las políticas de seguridad establecidas.

- **Implementación de Mejoras de Seguridad:** Aprovecha la oportunidad de la restauración para implementar mejoras de seguridad. Esto puede incluir la revisión y la actualización de políticas de seguridad, la implementación de medidas de seguridad adicionales y la capacitación del personal en mejores prácticas de seguridad.

- **Documentación de lecciones aprendidas:** Después de la restauración, es importante documentar las lecciones aprendidas del incidente. Esto incluye la revisión de lo sucedido, las medidas tomadas durante la respuesta y las acciones para evitar futuros incidentes similares.

- **Plan de Continuidad del Negocio:** Si la interrupción del incidente tuvo un impacto significativo en las operaciones del negocio, considera la implementación de un plan de continuidad del negocio para garantizar la operación ininterrumpida en caso de futuros incidentes.

- **Comunicación Post-Incidente:** Comunica internamente y, si es necesario, externamente sobre el incidente y la restauración exitosa. Asegúrate de que las partes interesadas estén al tanto de que se ha resuelto el incidente y de las medidas tomadas para proteger la organización en el futuro.

- **Informe y Documentación**

La "Informe y Documentación" es una fase crítica en la respuesta a un ataque informático, ya que implica la creación de registros detallados y documentación que respalden todas las acciones tomadas durante el incidente. Dentro de la documentación se detallan los siguientes pasos:

- **Registro de Incidentes:** Desde el inicio del incidente, es importante mantener un registro detallado de todos los eventos, acciones y observaciones relacionadas con el incidente. Esto incluye la hora y fecha de detección, la naturaleza del incidente, las partes involucradas, los sistemas afectados y cualquier otro detalle relevante.

- **Información de Contacto:** Mantén una lista actualizada de las personas y equipos de respuesta involucrados en la gestión del incidente, incluyendo sus nombres, roles, direcciones de correo electrónico y números de teléfono. Esto facilita la comunicación y la coordinación durante la respuesta.

- **Registro de Acciones Tomadas:** Documenta todas las acciones tomadas para identificar, mitigar y resolver el incidente. Esto incluye acciones técnicas, como el parcheo de sistemas, la restauración de copias de seguridad y la implementación de medidas de seguridad, así como acciones de comunicación, como notificaciones a partes interesadas.

- **Registro de Comunicaciones:** Mantén registros de todas las comunicaciones relacionadas con el incidente. Esto incluye correos electrónicos, mensajes de chat, llamadas telefónicas y cualquier otra forma de comunicación utilizada para coordinar la respuesta.

- **Registro de Decisiones:** Documenta todas las decisiones clave tomadas durante la respuesta al incidente, incluyendo quién las tomó, cuándo y por qué. Esto proporciona un contexto importante para futuras evaluaciones y revisiones.

- **Registro de Hallazgos:** Mantén un registro de todos los hallazgos relacionados con el incidente, incluyendo evidencia digital, registros de actividad sospechosa y cualquier otra información que respalde la narrativa del incidente.

- **Informe de Incidente:** Prepara un informe detallado del incidente una vez que se haya resuelto. Este informe debe incluir una descripción completa del incidente, los impactos sufridos, las medidas tomadas durante la respuesta y las lecciones aprendidas. También debe incluir recomendaciones para mejorar la seguridad en el futuro.

- **Diagramas y Gráficos:** Utiliza diagramas y gráficos para visualizar la secuencia de eventos y la propagación del incidente, especialmente si es un

incidente complejo. Esto puede ayudar a las partes interesadas a comprender mejor la situación.

- **Análisis Post-Incidente:** Realiza un análisis post-incidente para evaluar la eficacia de la respuesta y las áreas de mejora. Esto puede incluir la identificación de debilidades en los procedimientos de seguridad y recomendaciones para fortalecer la postura de seguridad.

- **Archivo Seguro:** Almacena todos los registros y documentos de manera segura en un lugar protegido. La seguridad de esta información es esencial para garantizar la integridad y la confidencialidad de los datos relacionados con el incidente.

- **Revisión y Actualización:** Revise y actualice regularmente los informes y documentos relacionados con incidentes a medida que se obtenga nueva información o se realicen mejoras en la respuesta a incidentes.

- **Mejoras en la Seguridad**

La fase de "Mejoras en la Seguridad" es crucial en el proceso de respuesta a incidentes de seguridad. Después de manejar el incidente actual, es esencial tomar medidas para fortalecer la seguridad y prevenir futuros incidentes similares. Las mejoras en la seguridad son esenciales para fortalecer la postura de seguridad de la organización y reducir la probabilidad de futuros incidentes. La seguridad de la información debe ser un enfoque constante y en evolución para proteger los activos de la organización.

- ✓ **¿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?**

El análisis BLUE TEAM se encuentra como adjunto en el .zip donde se da respuesta a este punto de la guía

- ✓ **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?**

Equipo	Función Principal	Tareas Clave	Enfoque
Blue Team[14]	Defensa y protección de sistemas y redes.	• Monitoreo de seguridad. • Detección y respuesta a amenazas. • Configuración y mantenimiento de firewalls, IDS/IPS. • Administración de parches y gestión de vulnerabilidades.	• Protección de activos y datos. • Mantenimiento de seguridad.
Red Team[15]	Pruebas de penetración y simulación de ataques.	• Ejecución de pruebas de penetración. • Identificación de vulnerabilidades. • Elaboración de informes de seguridad.	• Identificación de debilidades. • Evaluación de la postura de seguridad.
Purple Team[16]	Facilitar la colaboración entre Blue y Red Teams.	• Coordinación de ejercicios de seguridad. • Revisión de hallazgos de	• Mejora de la comunicación. • Transferencia de conocimientos.

[14] keepcoding. (21 de Febrero de 2023). [Sitio Web] KeepCoding Tech School. Obtenido de ¿Qué es Blue Team en Ciberseguridad? [consultado el 16 de Septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

[15] KeepCoding. (10 de Abril de 2023). [Sitio Web] KeepCoding Tech School. Obtenido de ¿Qué es Red Team en Ciberseguridad? [consultado el 16 de Septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

[16] KeepCoding. (21 de Julio de 2023). [Sitio Web] KeepCoding. Obtenido de KeepCoding Tech School [consultado el 16 de Septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/

		pruebas de penetración. • Identificación de debilidades y brechas en la seguridad.	
Csirt[17] (Equipo De Respuesta A Incidentes)	Responden y gestionan incidentes de seguridad.	• Detección y análisis de incidentes. • Coordinación de respuesta. • Comunicación con partes interesadas. • Análisis forense de incidentes.	• Respuesta y recuperación de incidentes. • Minimización del impacto. • Documentación de incidentes.

Tabla 1. Comparación entre Red Team, Blue Team, Purple Team y CSIRT

Fuente: Creación propia del estudiante

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

El Center for Internet Security (CIS) es una organización sin fines de lucro que desempeña un papel importante en el ámbito de la ciberseguridad, especialmente en apoyo a los equipos Blue Team y la mejora de la seguridad cibernética en general.

El CIS se dedica a promover mejores prácticas de seguridad cibernética y proporcionar recursos, herramientas y directrices que ayudan a las organizaciones y equipos Blue Team a fortalecer sus defensas y a mitigar amenazas cibernéticas. Las funciones principales de CIS incluyen:

- **Desarrollo de Pautas de Seguridad:** CIS crea y mantiene un conjunto de pautas de seguridad conocido como "CIS Controls" (Controles CIS) y "CIS Benchmarks" (Benchmarks CIS) que ofrecen directrices detalladas para proteger sistemas y redes contra amenazas comunes.

[17] SADVISOR. (05 de Septiembre de 2022). [Sitio Web] Security Advisor Su Defensa Digital. Obtenido de ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [consultado el 16 de Septiembre 2023]. Disponible en: https://sadvisor.com/que-es-el-csirt/

- **Investigación de Amenazas:** La organización realiza investigaciones sobre amenazas emergentes y vulnerabilidades de seguridad para proporcionar orientación actualizada a la comunidad de seguridad cibernética.

- **Capacitación y Concientización:** CIS ofrece capacitación y concientización en seguridad cibernética a través de recursos en línea, capacitación en persona y eventos de formación.

- **Evaluación y Certificación:** CIS ofrece programas de certificación para profesionales de seguridad cibernética y herramientas de evaluación de seguridad para medir y mejorar la postura de seguridad de una organización.

Dentro de las actividades y recursos ofrecidos por el Center for Internet Security (CIS), se pueden identificar varios enfoques o áreas clave, lo que podrías considerar como tipos de servicios o recursos proporcionados por CIS:

- **CIS Controls:** Los CIS Controls, anteriormente conocidos como "Critical Security Controls," son un conjunto de mejores prácticas de seguridad cibernética diseñadas para ayudar a las organizaciones a protegerse contra las amenazas más comunes. Estos controles se dividen en diferentes categorías y proporcionan pautas específicas para mejorar la seguridad de la red y los sistemas.

- **CIS Benchmarks:** Los CIS Benchmarks son guías de configuración detalladas para sistemas y aplicaciones específicas. Estas guías proporcionan instrucciones paso a paso sobre cómo configurar y endurecer sistemas operativos, aplicaciones y dispositivos para reducir las superficies de ataque y mejorar la seguridad.

- **CIS SecureSuite:** La CIS SecureSuite es una oferta de seguridad integral que incluye acceso a los CIS Controls y CIS Benchmarks, así como herramientas y recursos adicionales para ayudar a las organizaciones a evaluar y mejorar su postura de seguridad cibernética.

- **Capacitación y Concientización:** CIS ofrece programas de capacitación y concientización en seguridad cibernética para ayudar a las organizaciones y profesionales de seguridad a adquirir habilidades y conocimientos necesarios para proteger sus sistemas y redes.

- **Programas de Certificación:** CIS también ofrece programas de certificación en seguridad cibernética para profesionales que desean demostrar sus habilidades y conocimientos en el campo de la ciberseguridad.

CIS Workbench[18] es un recurso tecnológico donde es posible visualizar las configuraciones, estándares y buenas prácticas para la hardenizacion. por lo tanto, ayudan a determinar cómo fortalecer los sistemas de hardening. Para tener acceso a CIS Workbench es necesario tener una cuenta de la siguiente manera.

Ingresamos a la página https://workbench.cisecurity.org/ y damos en el botón registrarse ahora (*Ilustración* 18)

Ilustración 18. Registro en CIS WorkBench

Fuente: Creación propia del estudiante

Luego de eso ingresamos nuestros datos, aceptamos los términos y condiciones y damos en el botón registrar. (*Ilustración* 19)

[18] Security, C. C. (s.f.). [Sitio Web] CIS WorkBench. Obtenido de workbench Cisecurity [consultado el 16 de Septiembre 2023]. Disponible en: https://workbench.cisecurity.org/

Ilustración 19. Registro de datos Login

Fuente: Creación propia del estudiante

Al terminar el registro nos pedirá una verificación de nuestro email y después de esto nos pedirá los datos de ingreso. *(*Ilustración 20*)*

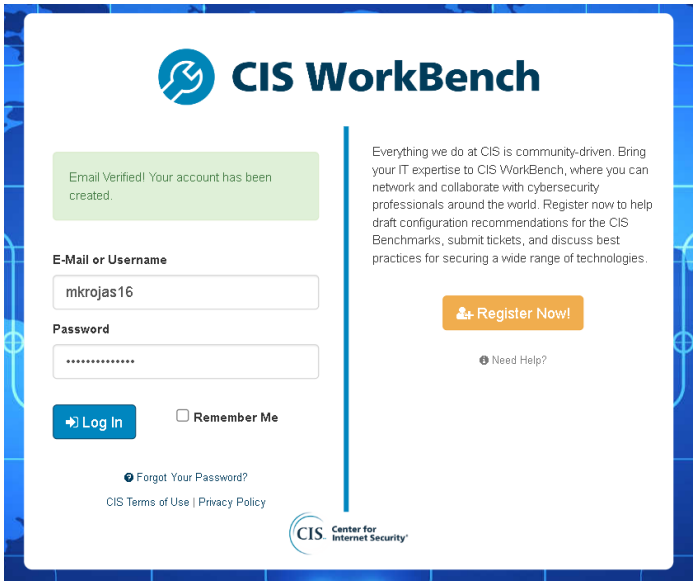

Ilustración 20. Ingreso y verificación de correo

Fuente: Creación propia del estudiante

Y con esto ya tendremos acceso a las referencias, archivos de descargas y foros de la comunidad disponibles en CIS Workbench. *(*Ilustración 21*)*

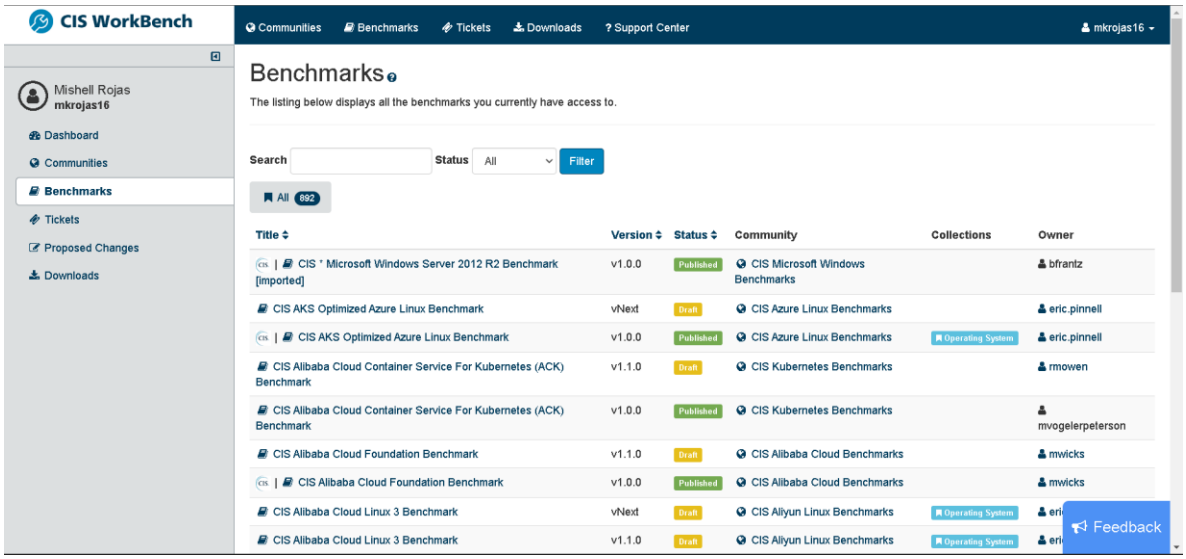

Ilustración 21. Acceso a CIS Workbench

Fuente: Creación propia del estudiante

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

Aspecto	SIEM[19]	XDR[20]
Definición	Un SIEM es una solución que recopila, correlaciona y analiza registros y eventos de seguridad de múltiples fuentes para proporcionar visibilidad y alertas sobre amenazas de seguridad.	XDR es una solución de seguridad cibernética que amplía la funcionalidad de detección y respuesta más allá de la infraestructura de seguridad tradicional, incluyendo endpoints, redes y aplicaciones.
Alcance De Detección	Principalmente enfocado en la detección y correlación de eventos de seguridad en logs y registros de dispositivos, aplicaciones y sistemas.	Ofrece detección avanzada y análisis de amenazas que abarca múltiples vectores de ataque, incluyendo endpoints, redes, correo

[19] IBM. (s.f.). [Sitio Web] IBM. Obtenido de ¿Qué es SIEM? [consultado el 16 de Septiembre 2023]. Disponible en: https://www.ibm.com/mx-es/topics/siem

[20] IBM. (s.f.). [Sitio Web] IBM. Obtenido de ¿Qué es XDR? [consultado el 16 de Septiembre 2023]. Disponible en: https://www.ibm.com/es-es/topics/xdr

		electrónico y cargas de trabajo en la nube.
Fuentes De Datos	Recopila datos de una amplia gama de fuentes, como firewalls, sistemas de detección de intrusiones (IDS/IPS), registros de servidores, logs de aplicaciones y más.	Adquiere datos de múltiples fuentes, incluyendo endpoints, sensores de red, registros de eventos, correo electrónico y más.
Correlación De Eventos	Realiza correlación de eventos y alertas basada en reglas predefinidas y patrones de comportamiento para identificar posibles amenazas.	Utiliza técnicas avanzadas de análisis y correlación para detectar amenazas persistentes y ataques sofisticados en tiempo real.
Respuesta A Incidentes	Proporciona funcionalidades básicas para la gestión de incidentes, como alertas y notificaciones, pero puede requerir integraciones adicionales para una respuesta efectiva.	Ofrece capacidades avanzadas de respuesta a incidentes, como la automatización de respuestas, la orquestación de seguridad y la capacidad de aislar endpoints comprometidos.
Visibilidad	Ofrece visibilidad limitada, principalmente a nivel de eventos y alertas de seguridad, con la necesidad de personalización y ajuste fino.	Proporciona una visión más completa y contextual de la infraestructura de seguridad y las amenazas en tiempo real, facilitando la comprensión de la magnitud de un incidente.
Implementación	Puede requerir una implementación compleja y personalización significativa para adaptarse a las necesidades específicas de la organización.	Suele ofrecer una implementación más rápida y sencilla, ya que integra múltiples fuentes de datos y proporciona capacidades de análisis avanzadas de manera nativa.
Enfoque De Plataforma	Por lo general, no se considera una plataforma	Se concibe como una plataforma unificada que

de seguridad integral, sino más bien una herramienta de monitoreo y detección.	aborda de manera integral la detección, respuesta y neutralización de amenazas en toda la organización.

Tabla 2. Diferencia ente SIEM y XDR

Fuente: Creación propia del estudiante

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

- **Snort[21]:** Snort es una de las herramientas de detección de intrusiones de red (NIDS) más populares y ampliamente utilizadas. Funciona analizando el tráfico de red en busca de patrones de comportamiento y firmas de ataques conocidas. Snort permite la detección de una amplia variedad de amenazas, incluyendo ataques de intrusión, malware y ataques de denegación de servicio (DoS). También es altamente personalizable y extensible a través de reglas personalizadas.

- **Suricata[22]:** Suricata es otra herramienta de detección de intrusiones de red (NIDS) de código abierto que ofrece capacidades de análisis avanzado de tráfico de red. Está diseñado para ser rápido y eficiente. Suricata es capaz de realizar análisis en tiempo real de tráfico de red en busca de amenazas, incluyendo ataques de red y malware. Ofrece soporte para reglas de detección personalizadas y es compatible con varios formatos de registro.

- **OSSEC[23]:** OSSEC es una plataforma de seguridad de código abierto que combina detección de intrusiones, registro de seguridad, análisis de registro y respuesta a incidentes en una sola solución. Puede utilizarse tanto como un sistema de prevención de intrusiones de host (HIPS) como un sistema de detección de intrusiones de host (HIDS). OSSEC monitorea y analiza registros y eventos de seguridad en sistemas operativos y aplicaciones para detectar comportamientos anómalos o posibles intrusiones. También ofrece

[21] SNORT. (s.f.). [Sitio Web] SNOR. Obtenido de Firewall Snort [consultado el 16 de Septiembre 2023]. Disponible en: https://www.snort.org/

[22] SURICATA. (s.f.). [Sitio Web] SURICATA. Obtenido de Firewall Suricata [consultado el 16 de Septiembre 2023]. Disponible en: https://suricata.io/

[23] OSSEC. (s.f.). [Sitio Web] OSSEC. Obtenido de FIrewall Ossec [consultado el 16 de Septiembre 2023]. Disponible en: https://www.ossec.net/

capacidades de respuesta a incidentes, como notificaciones y ejecución de scripts personalizados.

6 Etapa 4 análisis blue team

Configuración de Firewall de Windows

Para mitigar y prevenir el ataque que se obtuvo mediante el payload lo primero que debemos hacer es habilitar el registro de paquetes descartados, esta una configuración en el firewall que determina si se debe registrar información sobre los paquetes de red que son bloqueados o descartados por el firewall. Es importante destacar que el registro de paquetes descartados puede proporcionar información valiosa para la seguridad y el monitoreo de la red, también genera grandes cantidades de datos. (*Ilustración* 22)

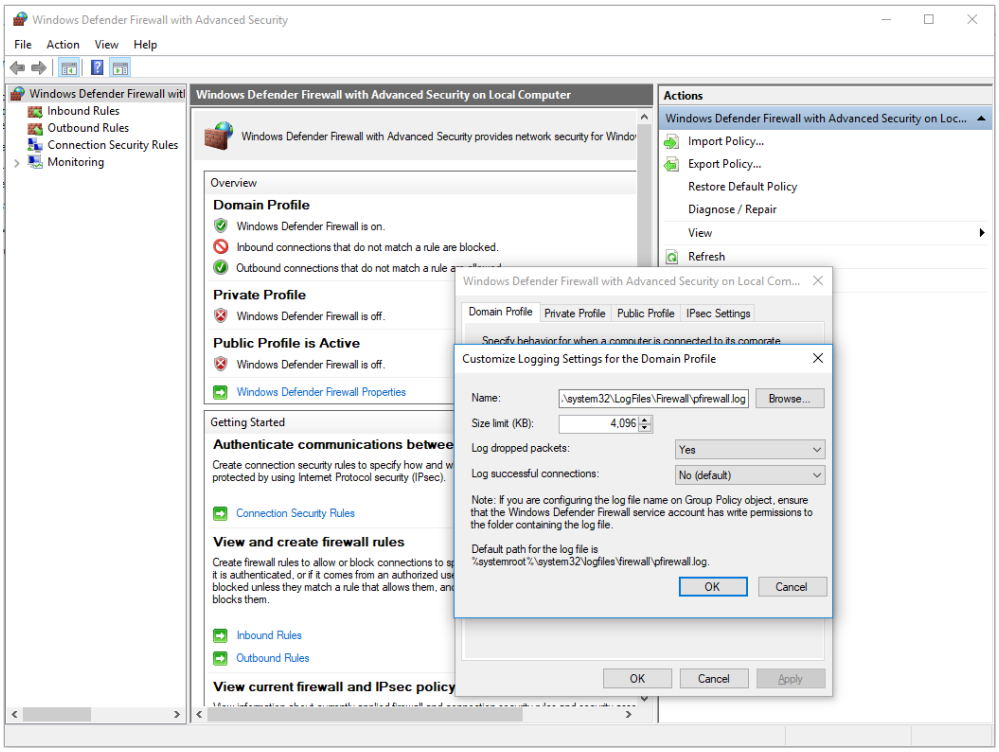

Ilustración 22 habilitar el registro de paquetes descartados

Fuente: Creación propia del estudiante

Luego procedemos con desactivar la aplicación de reglas locales y desactivar las notificaciones que es una configuración en el firewall que permite deshabilitar temporalmente la aplicación de reglas de seguridad locales y las notificaciones asociadas. Esta configuración puede reducir la seguridad de un sistema o red. (*Ilustración* 23)

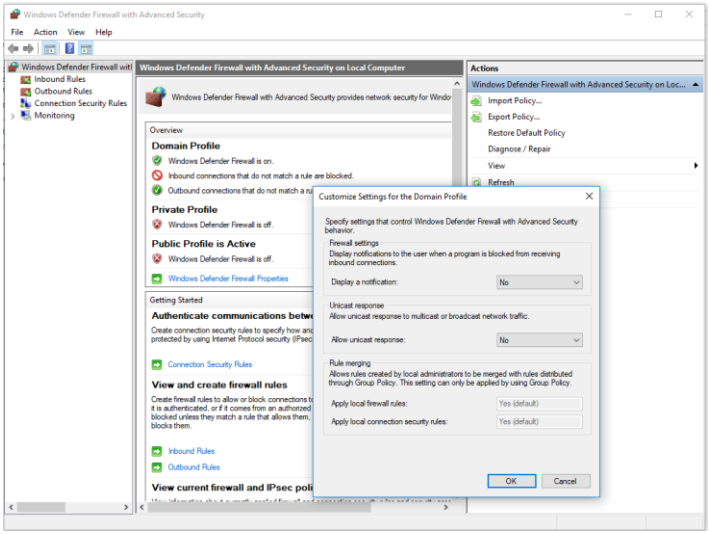

Ilustración 23 desactivar la aplicación de reglas locales y desactivar las notificaciones

Fuente: Creación propia del estudiante

Lo siguiente que hacemos es bloquear conexiones salientes por defecto, esto configura sus reglas de forma predeterminada para bloquear todas las conexiones que intentan salir de la red o del sistema, a menos que se especifique lo contrario mediante reglas específicas de permisos. (*Ilustración* 24)

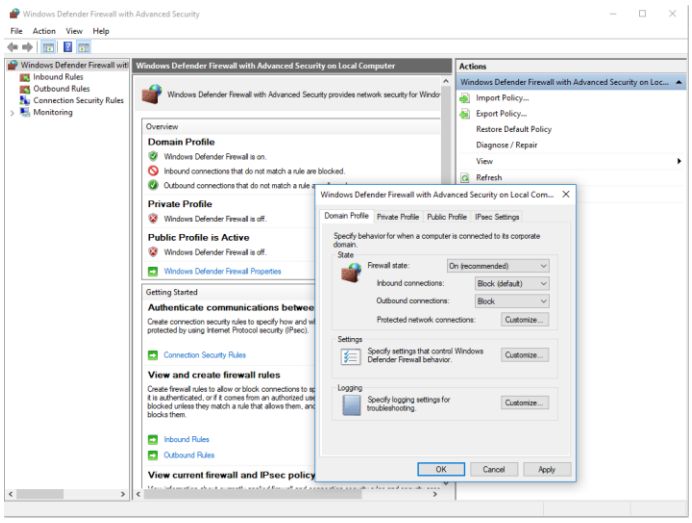

Ilustración 24 bloquear conexiones salientes por defecto

Fuente: Creación propia del estudiante

Configuración de las Reglas para Servicios Necesarios

Luego de haber bloqueado todas las conexiones salientes en el firewall debemos realizar las configuraciones para todos los servicios necesarios para la compañía y para esto debemos crear una regla customizada en el firewall de Windows. (*Ilustración* 25)

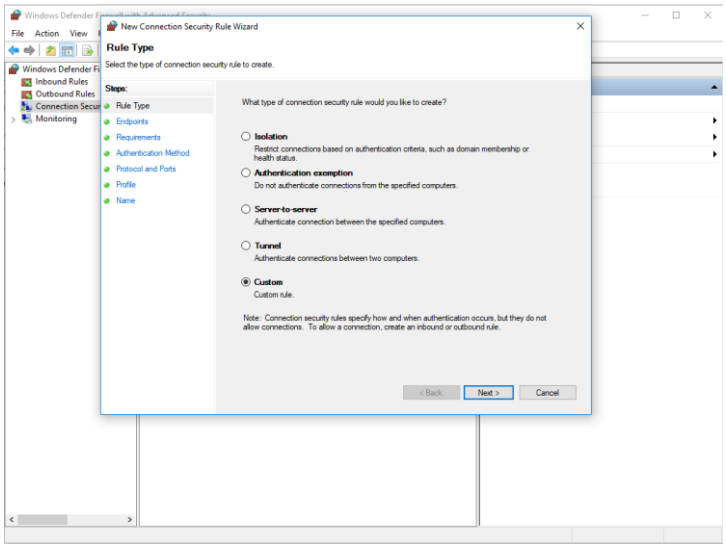

Ilustración 25 configuración de reglas

Fuente: Creación propia del estudiante

En la configuración de la regla debemos colocar la IP del endpoint de entrada y de salida que vamos a utilizar y a permitir el tráfico a través del firewall. (*Ilustración* 26)

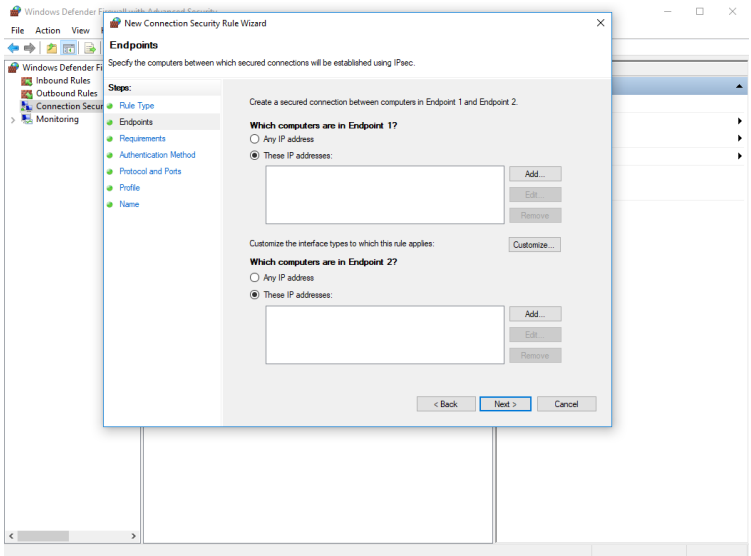

Ilustración 26 Agregar las IP

Fuente: Creación propia del estudiante

Además de colocar las IP's de los endpoing es necesario colocar un método de autenticación para los endpoints y seleccionamos la autenticación tanto para los de entrada como para los de salida. (*Ilustración* 27)

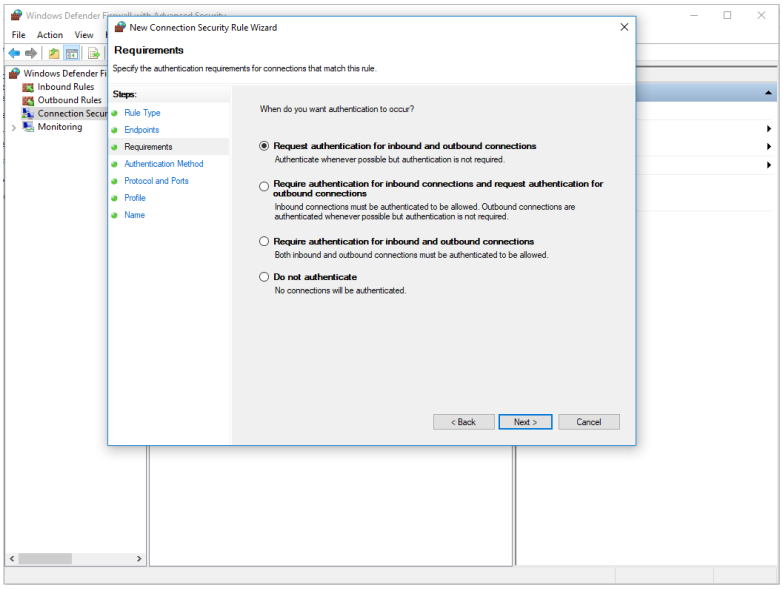

Ilustración 27 Agregar autenticación

Fuente: Creación propia del estudiante

Por defecto Windows nos ofrece como método de autenticación Kerberos V5 que es el método de autenticación que vamos a utilizar para la conexión del endpoint en nuestra regla. (Ilustración 28)

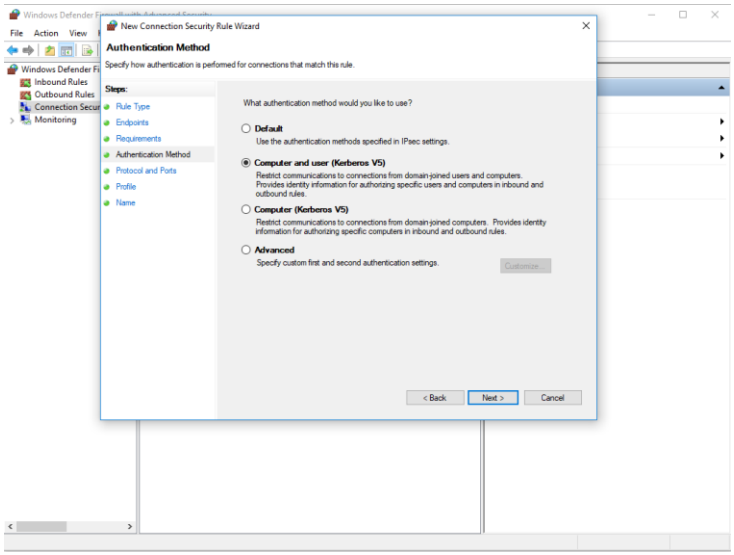

Ilustración 28 Seleccionar autenticación

Fuente: Creación propia del estudiante

Y por último seleccionamos los puertos que van a ser utilizados por el endpoint para la conexión para que sean los puertos que van a estar abiertos para el tráfico seguro. (*Ilustración* 29)

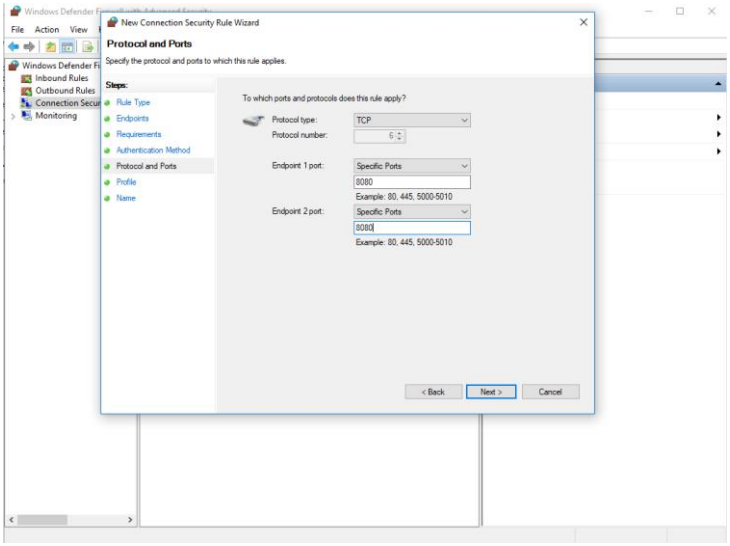

Ilustración 29 Selección de puertos

Fuente: Creación propia del estudiante

Ahora vamos a agregar excepciones a servicios básicos, como Windows Update y Microsoft Defender para que permita el acceso y el funcionamiento ininterrumpido de servicios críticos o esenciales, incluso cuando se aplican reglas de seguridad más estrictas.

Esta práctica es importante al bloquear todas las peticiones salientes se puede afectar negativamente el funcionamiento de servicios fundamentales o actualizaciones de seguridad. (*Ilustración* 30)

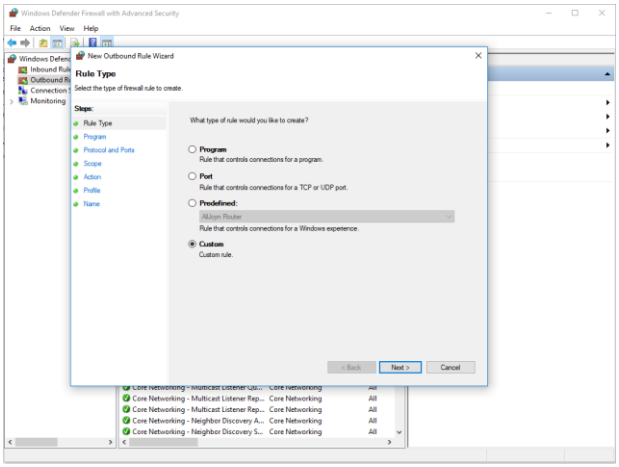

Ilustración 30 Creación de reglas de salida

Fuente: Creación propia del estudiante

En la siguiente ventana debemos colocar cual es el servicio al que se le va a permitir el tráfico, en este caso es svchost.exe pero también se debe hacer para el servicio smartscreen.exe estos dos nos permiten evitar que se inhabiliten servicios como Windows defender, Windows update, ntivirus Network Inspection Service, Antivirus Network Inspection Service entre otros. (*Ilustración* 31)

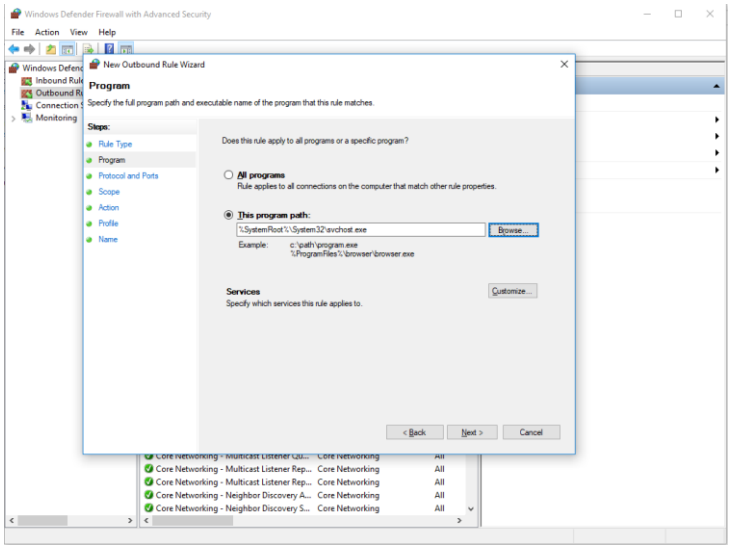

Ilustración 31 Se agregan los servicios

Fuente: Creación propia del estudiante

Ahora seleccionamos el protocolo por el cual se va a hacer la conexión y los puertos que se van a utilizar para no entorpecer el funcionamiento de los servicios de Windows. (*Ilustración* 32)

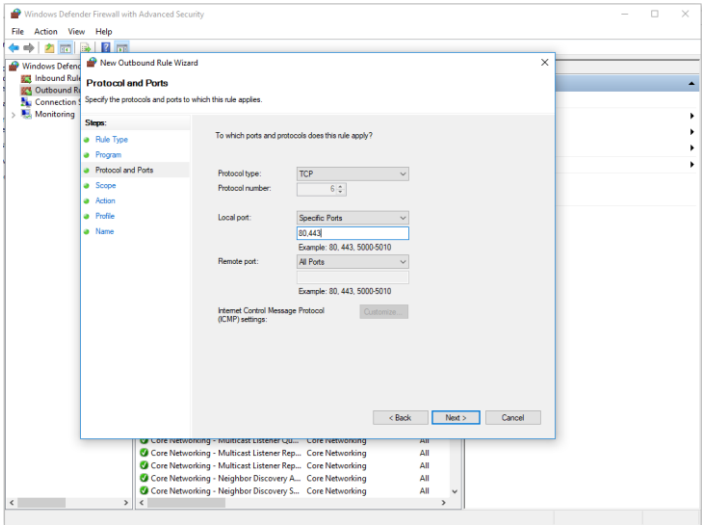

Ilustración 32 Se configuran los puertos

Fuente: Creación propia del estudiante

Y por último permitimos todas las conexiones para estos servicios. (*Ilustración* 33)

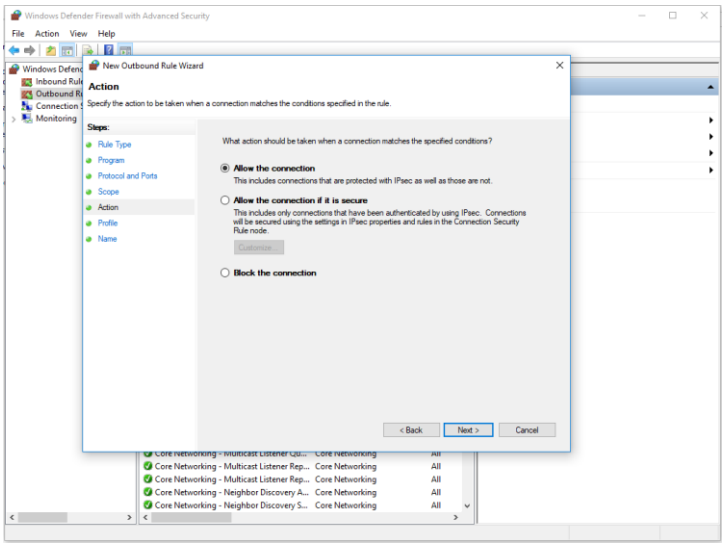

Ilustración 33 Se permiten las conexiones

Fuente: Creación propia del estudiante

Loggin

Además de configurar las políticas del firewall, se debe realizar configuraciones en el Audit Policy para tener un log de cada vez que se intente alguien loggearse en el sistema sea que lo logre o que no logre hacerlo para poder tener alertas en el caso de que alguien no logre acceder al sistema de forma repetida. (Ilustración 34)

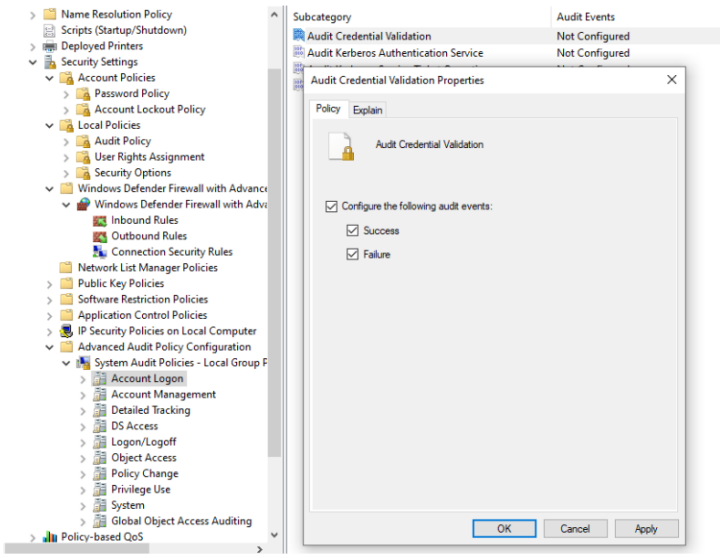

Ilustración 34 Audit Log

Fuente: Creación propia del estudiante

7 Etapa 5 socialización de informe técnico

- **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 una organización puede ser una estrategia efectiva para fortalecer la ciberseguridad y mejorar la capacidad de detección y respuesta ante amenazas cibernéticas. Cada equipo tiene un papel específico en este enfoque, y trabajar juntos puede mejorar la postura de seguridad de la organización de varias maneras como, por ejemplo:
En la detección temprana de amenazas el equipo Blue Team se encarga de monitorear y defender la red y los sistemas de la organización. Trabajando en estrecha colaboración con el equipo Red Team, pueden aprender de las tácticas y técnicas utilizadas por los atacantes simulados. Esto les permite mejorar la detección de amenazas y ajustar las defensas en función de las vulnerabilidades identificadas durante los ejercicios de Red Team.

Durante la validación de la efectividad de las defensas el equipo Red Team simula ataques reales para evaluar la eficacia de las defensas de la organización. Al hacerlo, pueden identificar debilidades en las políticas de seguridad, la configuración de sistemas y la capacitación del personal. Trabajando con el equipo Blue Team, se pueden corregir estas debilidades de manera proactiva.
La colaboración entre los equipos Blue Team y Red Team permite un flujo constante de información sobre las amenazas y las tácticas utilizadas en el mundo real. Esto permite que el equipo Blue Team esté mejor preparado para identificar y responder a amenazas en tiempo real y fomentando el aprendizaje continuo.

En la mejora de políticas y procedimientos la retroalimentación constante entre los equipos Blue Team y Red Team puede ayudar a la organización a desarrollar y ajustar sus políticas y procedimientos de seguridad. Esto incluye la revisión de políticas de acceso, la gestión de parches y actualizaciones, y la capacitación del personal en temas de seguridad.

El equipo Purple Team actúa como intermediario entre los equipos Blue y Red. Su función es coordinar los ejercicios, facilitar la comunicación y asegurarse de que se aprendan lecciones de cada ejercicio. El equipo Purple Team puede ayudar a definir los objetivos del Red Team y garantizar que los Blue Team estén listos para responder y tomar medidas correctivas.

La integración de estos equipos fomenta una cultura de seguridad más sólida dentro de la organización. Los empleados aprenden a estar más atentos a las amenazas cibernéticas y a tomar medidas proactivas para proteger la información y los sistemas de la empresa. Trabajar juntos en ejercicios de Red Team y Purple Team

ayuda a la organización a estar mejor preparada para gestionar incidentes de seguridad reales. El personal de Blue Team adquiere experiencia en la detección y respuesta a amenazas, lo que puede ser crucial en caso de un ciberataque real y ayuda a estar preparado para cualquier incidente inesperado.

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

El establecimiento de políticas de seguridad y la implementación de recomendaciones efectivas son fundamentales para mejorar la ciberseguridad en cualquier organización en sus entornos de Tecnologías de la Información (TI). A continuación, se presentan algunas políticas y recomendaciones:

- ✓ **Política de acceso y autenticación:** Dentro de las políticas de acceso y autenticación se establecen normas de cambio periódicos de contraseñas y para la creación de contraseñas más fuertes y seguras además de la implementación de autenticación multifactor (MFA/2FA) como un mandato para el acceso a sistemas críticos y redes. Otro punto clave en las políticas de acceso es la gestión de las cuentas de usuario, donde se establecen procedimientos para agregar, modificar y deshabilitar las cuentas de manera segura.

- ✓ **Política de seguridad de datos:** Las políticas de seguridad de datos incluyen la clasificación de datos para definir categorías y aplicar las medidas de seguridad proporcionales a su sensibilidad, el cifrado de datos en reposo y tránsito, especialmente en dispositivos móviles y en la nube. Además de políticas de retención de datos y directrices para el almacenamiento y eliminación segura de datos obsoletos.

- ✓ **Política de seguridad de red:** Las políticas de seguridad de rec incluyen la implementación de firewall y filtrado de contenido para proteger la red contra las amenazas externas, la segmentación de red para limitar el movimiento lateral de los atacantes, el monitoreo de red para monitorizar y detectar actividades sospechosas y alertar a tiempo.

- ✓ **Política de gestión de parches y actualizaciones:** La implementación de políticas de actualización regular para mantener los sistemas, aplicaciones y dispositivos con los últimos parches de seguridad, la creación de programas

de gestión de parchas para establecer pruebas y seguimiento de las implementaciones de parches y evitar errores.

- ✓ **Política de capacitación y concientización:** Las políticas de capacitación incluyen entrenamientos en seguridad para proporcionar capacitación en seguridad informática a todos los empleados para reconocer amenazas y practicas seguras, además la realización de pruebas de phishing simulado para evaluar la preparación de los empleados y brindar retroalimentación.

- ✓ **Política de gestión de incidentes:** Los planes de respuesta a incidentes incluyen los pasos a seguir, las notificación y roles y responsables claros, también el registro y reporte de incidentes que establecen los procedimientos claros para la respuesta de manera oportuna, esto son parte de la política de gestión de incidentes.

- ✓ **Política de terceros y proveedores:** Dentro de las políticas de terceros se establece la evaluación de los proveedores para seleccionar los servicios basados en su seguridad informática y su infraestructura, además de la inclusión de cláusulas de seguridad en acuerdos contractuales con terceros.

- ✓ **Política de gestión de dispositivos móviles:** Políticas Bring Your Own Device para la gestión segura de dispositivos personales que acceden a recursos de la organización y controles de aplicaciones para limitar el uso de aplicaciones no autorizadas en dispositivos corporativos.

- ✓ **Política de auditoría y cumplimiento:** Realizar auditorías regulares de seguridad interna y externa para evaluar el cumplimiento de las políticas, realizar seguimiento estableciendo procesos de corrección y evaluación de cumplimiento de políticas.

- ✓ **Política de continuidad del negocio y recuperación ante desastres:** Desarrollar planes de continuidad del negocio y de recuperación ante desastres para mantener la operatividad en caso de incidentes graves.

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

La ciberseguridad se ha convertido en una preocupación crítica para las organizaciones en la era digital actual. Los ciberataques son cada vez más sofisticados y pueden causar daños significativos en términos de pérdida de datos, interrupción de operaciones y daño a la reputación de la empresa. En este contexto, el reciente curso dedicado a la ciberseguridad proporcionó información valiosa que respalda la necesidad de inversiones estratégicas en esta área.

Uno de los aspectos más destacados del seminario fue la realización de pruebas de red team, una metodología que simula ataques cibernéticos reales para evaluar la seguridad de una organización. Durante estas pruebas, como expertos en seguridad se recrearon situaciones en las que se encontraron vulnerabilidades críticas. En particular, se identificaron fallas de seguridad relacionadas con la escalada de permisos y el acceso remoto a un sistema Windows.

En el caso de la escalada de permisos, los atacantes potenciales lograron explotar debilidades en la configuración de privilegios de usuario para elevar sus permisos a niveles más altos de privilegio. Esto es especialmente peligroso, ya que permite a un atacante acceder a información sensible y realizar cambios en sistemas críticos. Además, se detectaron vulnerabilidades en la gestión del acceso remoto a sistemas Windows. Los atacantes demostraron la posibilidad de obtener acceso no autorizado a través de métodos como la suplantación de identidad (spoofing) y la explotación de debilidades en la autenticación.

La respuesta del equipo Blue Team a estos hallazgos fue fundamental. Se implementaron medidas de mitigación inmediatas, como la mejora de las políticas de seguridad, la implementación de controles de acceso más estrictos y la revisión de la gestión de privilegios. Además, se estableció un sistema de monitoreo de seguridad en tiempo real para detectar y responder a cualquier intento de escalada de permisos o acceso no autorizado.

Un aspecto importante que se consideró en este proceso fue la revisión de la legislación colombiana en materia de ciberseguridad, específicamente la Ley 1273 de 2009. Esta ley establece disposiciones relacionadas con la protección de la información y la lucha contra los delitos informáticos en Colombia. Sirvió como base legal sólida para respaldar las políticas y prácticas de seguridad cibernética implementadas por la organización, garantizando así su cumplimiento con los estándares legales locales.

En resumen, el curso y las pruebas de red team proporcionaron evidencia clara y convincente de la necesidad de inversiones en ciberseguridad. Los hallazgos de vulnerabilidades graves y las técnicas utilizadas en estos ataques simulados subrayaron la urgencia de fortalecer la infraestructura de seguridad de la organización. La implementación de medidas de mitigación y respuesta, así como el cumplimiento de la legislación colombiana pertinente, se convirtieron en pasos críticos hacia la protección de activos y la conformidad con los estándares legales.

Al presentar estas conclusiones respaldadas por pruebas concretas y análisis legal, la alta gerencia estará mejor informada sobre la importancia de la inversión en ciberseguridad y será más propensa a tomar decisiones que protejan los activos y la reputación de la organización.

- **Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video.**

Enlace del video de sustentación: Sustentación Etapa 5_Mishell Rojas.mp4

- **Resultado de prueba anti plagio**

Enlace del resultando de Turnitin: Etapa 5_Turnitin.pdf

Conclusiones

Durante el desarrollo del curso se abordaron una serie de aspectos relacionados con la ciberseguridad y la protección de datos en Colombia. comenzando con una revisión de la legislación colombiana, resaltando las leyes 1273 de 2009 y 1581 de 2012 que rigen la protección de datos y los delitos informáticos, junto con las sanciones y la entidad reguladora. Luego, se exploraron temas como la ética en la ciberseguridad, análisis de incidentes de cibercrimen y la importancia de una respuesta efectiva a las amenazas cibernéticas.

En la segunda etapa, se evaluó un acuerdo de confidencialidad y se destaca su conformidad con la Ley 1581, señalando deficiencias legales y éticas. También se discutió el cumplimiento ético de aceptar contratos que violen los estándares éticos y legales.

La tercera etapa involucro un ejercicio de Red Team para evaluar la seguridad de una empresa y se subraya la importancia de mantener defensas actualizadas y resilientes.

Finalmente, la cuarta etapa, se enfoca en la identificación y respuesta a amenazas cibernéticas, haciendo hincapié en la necesidad de seguir una serie de pasos clave. También se menciona la utilidad de recursos como el Center for Internet Security (CIS).

Recomendaciones

- **Revisión Legal Rigurosa:** Antes de aceptar cualquier acuerdo de confidencialidad o contrato, es fundamental llevar a cabo una revisión exhaustiva de sus términos y condiciones. Esto debe incluir la consulta con expertos legales para asegurarse de que el acuerdo cumpla con todas las leyes y regulaciones aplicables, especialmente en lo que respecta a la protección de datos personales y la ciberseguridad.

- **Claridad en el Tratamiento de Datos:** Los acuerdos de confidencialidad deben definir de manera clara y específica cómo se manejarán los datos personales, incluyendo cómo se recopilarán, almacenarán, procesarán y protegerán. Deben seguir los principios establecidos en las leyes de protección de datos pertinentes, como la Ley 1581 de Colombia.

- **Consentimiento Informado:** Es imperativo obtener el consentimiento informado de las personas cuyos datos personales se recopilarán y procesarán. Esto debe ser una práctica estándar y estar documentada de acuerdo con la legislación aplicable.

- **Derechos de los Titulares de Datos**: El acuerdo debe establecer explícitamente cómo se respetarán y garantizarán los derechos de los titulares de datos, incluyendo el acceso, rectificación, actualización y supresión de la información personal. Esto es fundamental para cumplir con la Ley 1581.

- **Medidas de Seguridad:** El acuerdo debe detallar las medidas de seguridad técnicas, administrativas y físicas que se implementarán para proteger la información personal. Esto es esencial para cumplir con los requisitos de seguridad establecidos en la legislación.

- **Registro de Bases de Datos**: Si corresponde, asegúrese de que el acuerdo contemple el registro de las bases de datos en el Registro Nacional de Bases de Datos, como lo exige la Ley 1581 en Colombia.

- **Educación en Seguridad Cibernética:** Promueva la educación en seguridad cibernética tanto en la organización como entre los usuarios finales. La prevención es clave para evitar caer en estafas y fraudes cibernéticos, como el caso de los códigos QR mencionados.

- **Denuncia de Delitos Cibernéticos:** En caso de encontrar o ser víctima de un delito cibernético, se debe denunciar a las autoridades pertinentes y proporcionar toda la información relevante para ayudar en la investigación.

- **Cumplimiento Ético:** Como profesional en ciberseguridad, es esencial seguir los principios éticos y legales establecidos por su organización y las autoridades competentes. Si un acuerdo o contrato viola estos principios, debe rechazarse y, si es necesario, denunciarse.

- **Actualización Constante:** Manténgase actualizado sobre las últimas tendencias y amenazas en el campo de la ciberseguridad. La evolución tecnológica requiere una constante adaptación y aprendizaje para mantenerse seguro y proteger la información.

- **Aplicación de Parches y Actualizaciones de Seguridad:** Priorice y aplique los parches de seguridad críticos en todos los sistemas y servidores afectados lo antes posible para abordar las vulnerabilidades identificadas. Esto debe hacerse de manera regular y sistemática.

- **Auditorías de Seguridad Continuas:** Implemente auditorías de seguridad regulares en su infraestructura y aplicaciones para detectar y remediar nuevas vulnerabilidades. Esto garantizará una postura de seguridad proactiva.

- **Educación en Seguridad para el Personal:** Proporcione capacitación en seguridad cibernética a todos los miembros del personal para aumentar la conciencia sobre la importancia de prácticas seguras, contraseñas robustas y la detección de posibles amenazas.

- **Gestión Efectiva de Parches:** Establezca un proceso de gestión de parches efectivo que incluya la revisión y aplicación regular de actualizaciones críticas. Monitoree el estado de parcheo de todos los sistemas.

- **Monitorización Continua de Eventos de Seguridad:** Implemente un sistema de monitorización de eventos de seguridad que detecte y responda a actividades inusuales o sospechosas en tiempo real. Esto ayudará a identificar y mitigar amenazas de manera más rápida.

- **Evaluación Regular de la Infraestructura:** Realice evaluaciones periódicas de seguridad en toda su infraestructura y aplicaciones para identificar y abordar nuevas vulnerabilidades antes de que los atacantes puedan explotarlas.

- **Actualización de Políticas y Procedimientos de Seguridad**: Revise y actualice regularmente las políticas y procedimientos de seguridad cibernética para asegurarse de que reflejen las mejores prácticas y estén al día con las amenazas emergentes.

- **Ejercicios de Concienciación en Seguridad:** Realice ejercicios regulares de concienciación en seguridad para educar a su personal sobre las mejores prácticas de seguridad y cómo identificar posibles ataques de ingeniería social.

- **Plan de Respuesta a Incidentes:** Desarrolle y mantenga un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad. Asegúrese de que todo el personal esté familiarizado con este plan.

- **Auditorías Externas:** Considere la posibilidad de realizar auditorías de seguridad externas periódicas realizadas por profesionales de seguridad independientes para obtener una evaluación objetiva de la seguridad de su empresa.

- **Seguimiento de Cumplimiento:** Asegúrese de cumplir con las regulaciones y estándares de seguridad relevantes para su industria, como GDPR, HIPAA, ISO 27001, etc. Esto garantiza que esté al día con las mejores prácticas de seguridad.

- **Restablecimiento de Contraseñas y Análisis de Actividad:** Dado que se sospecha que se ha producido una violación, cambie todas las contraseñas y realice un análisis exhaustivo de la actividad del sistema para identificar cualquier actividad maliciosa adicional.

- **Políticas de Descarga y Ejecución de Software**: Establezca políticas estrictas sobre la descarga y ejecución de software en las computadoras de la empresa. Los empleados deben estar capacitados para identificar y evitar software no confiable.

- **Monitoreo de Tráfico de Red:** Implemente un sistema de monitoreo de tráfico de red para detectar y bloquear actividades sospechosas en la red, como el acceso no autorizado a través de puertos inusuales.

- **Restauración Segura de Sistemas:** Antes de volver a poner en línea los sistemas afectados, asegúrese de que estén completamente limpios y que todas las vulnerabilidades se hayan abordado. Realice un seguimiento constante de la actividad en busca de intrusiones posteriores.

Referencias bibliográficas

IBM. (s.f.). [Sitio Web] IBM. Obtenido de ¿Qué es SIEM? [consultado el 16 de Septiembre 2023]. Disponible en: https://www.ibm.com/mx-es/topics/siem

IBM. (s.f.). [Sitio Web] IBM. Obtenido de ¿Qué es XDR? [consultado el 16 de Septiembre 2023]. Disponible en: https://www.ibm.com/es-es/topics/xdr

OSSEC. (s.f.). [Sitio Web] OSSEC. Obtenido de FIrewall Ossec [consultado el 16 de Septiembre 2023]. Disponible en: https://www.ossec.net/

SNORT. (s.f.). [Sitio Web] SNOR. Obtenido de Firewall Snort [consultado el 16 de Septiembre 2023]. Disponible en: https://www.snort.org/

SURICATA. (s.f.). [Sitio Web] SURICATA. Obtenido de Firewall Suricata [consultado el 16 de Septiembre 2023]. Disponible en: https://suricata.io/

keepcoding. (21 de Febrero de 2023). [Sitio Web] KeepCoding Tech School. Obtenido de ¿Qué es Blue Team en Ciberseguridad? [consultado el 16 de Septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

KeepCoding. (10 de Abril de 2023). [Sitio Web] KeepCoding Tech School. Obtenido de ¿Qué es Red Team en Ciberseguridad? [consultado el 16 de Septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

KeepCoding. (21 de Julio de 2023). [Sitio Web] KeepCoding. Obtenido de KeepCoding Tech School [consultado el 16 de Septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/

Security, C. C. (s.f.). [Sitio Web] CIS WorkBench. Obtenido de workbench Cisecurity [consultado el 16 de Septiembre 2023]. Disponible en: https://workbench.cisecurity.org

publica, D. a. (18 de Octubre de 2012) . [Sitio Web]. Funcion Publica. Obtenido de Ley 1581 de 2012. . [consultado el 07 de Octubre 2023]. Diponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Colombia, R. d. (5 de Enero de 2009). [Sitio Web]. SIC. Obtenido de LEY 1273 DE [consultado el 07 de Octubre 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

NOWAK, S. (28 de Noviembre de 2022). [Sitio Web]. nuclio. Obtenido de ¿Qué es el Pentesting? [consultado el 07 de Octubre 2023]. Disponible en: https://nuclio.school/que-es-el-pentesting/

Hernández, M. (21 de Marzo de 2022). [Sitio Web]. ciberseguridad bidaidea. Obtenido de ¿Cuál son la 5 Fases del Pentesting? [consultado el 07 de Octubre 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

ciberseguridad. (s.f.). [Sitio Web]. ciberseguridad. Obtenido de ¿QUÉ ES CVE? EXPLICACIÓN DE LAS VULNERABILIDADES Y EXPOSICIONES COMUNES [consultado el 07 de Octubre 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

wikipedia. (12 de Julio de 2023). [Sitio Web]. wikipedia. Obtenido de Common Vulnerabilities and Exposures [consultado el 07 de Octubre 2023]. Disponible en: https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Exploit. (s.f.). *ExploitDB*. [Sitio Web]. Obtenido de Exploit DataBase [consultado el 07 de Octubre 2023]. Disponible en: https://www.exploit-db.com/

COPNIA. (2015). [Sitio Web]. Código de ética. Obtenido de Consejo Profesional Nacional de Ingenieria [consultado el 15 de Agosto 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Espectador, R. T. (21 de Enero de 2022). [Sitio Web]. ¡Cuidado! Delincuentes están usando códigos QR para estafar a sus víctimas. Obtenido de EL ESPECTADOR

[consultado el 15 de Agosto 2023]. Disponible en: https://www.elespectador.com/tecnologia/cuidado-delincuentes-estan-usando-codigos-qr-para-estafar-a-sus-victimas/

Colombia, R. d. (5 de Enero de 2009). [Sitio Web]. SIC. Obtenido de LEY 1273 DE 2009 [consultado el 07 de Octubre 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Publica, D. a. (18 de Octubre de 2012) . [Sitio Web]. función Pública. Obtenido de Ley 1581 de 2012. . [consultado el 07 de Octubre 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Flu-Project. (s.f.). RID Hijacking en Windows 10: [Sitio Web] ¿Qué es y cómo aprovecharlo? #Metasploit #Pentesting. Obtenido de Flu-Project [consultado el 08 de Septiembre 2023]. Disponible en: https://www.flu-project.com/2018/05/rid-hijacking-en-windows-10-que-es-y.html

Pérez, P. G. (s.f.). Hacking Windows 10: [Sitio Web] Escalada De Privilegios Con CVE-2019-0841. Obtenido de Hacking [consultado el 08 de Septiembre 2023]. Disponible en: https://www.hacking.land/2019/04/hacking-windows-10-escalada-de.html?m=1

SADVISOR. (05 de Septiembre de 2022). [Sitio Web] Security Advisor Su Defensa Digital. Obtenido de ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [consultado el 16 de Septiembre 2023]. Disponible en: https://sadvisor.com/que-es-el-csirt/

LIFARS. (noviembre de 2020). [Sitio Web] Guide to Hardening Windows 10 For Administrators, Developers and Office Workers. Obtenido de Lifars [consultado el 19 de Septiembre 2023]. Disponible en: https://lifars.com/wp-content/uploads/2020/11/Guide-to-Hardening-Windows-10.pdf