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

JAVIER ALBERTO MERCHAN

Nombre

JOHN FREDDY QUINTERO TAMAYO

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

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

JAVIER ALBERTO MERCHAN

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

CONTENIDO

GLOSARIO

Políticas De Seguridad: Son astutos que se rigen por procedimientos que aseguran la información de carácter privado de una empresa.

Protección: Es una actividad en la cual se protege a la información en un sistema de información dentro de lo cual se valida la información.

Cláusula: Condición en la cual se establece una condición o procedimiento del contrato

Hacker: Es una persona que ejecuta un taque informático cuya misión es sustraer información para diversos fines

Dato: Información almacenada de forma digital en un sistema informático

Blue Team: Es un grupo especializado de personas que están capacitadas en la gestión de controles de seguridad dentro de una compañía con los sistemas de protección de la información.

Red Team: Es un grupo especializado que realiza simulaciones de ataque en una red a través de diversos sistemas de penetración a la seguridad de la información dentro de una compañía teniendo en cuenta los protocolos de seguridad e la información.

Pentesting: Es un ataque simulado para un sistema de información que tiene como objetivo analizar las posibles vulnerabilidades de seguridad en el cual se valida la información más relevante para solucionar los posibles errores del manejo de la información.

Información: Es el conjunto de datos que se le realiza un proceso de modificación o almacenamiento dentro de un sistema informático, validando su destino final

INTRODUCCIÓN

Partiendo de que la informática involucra una serie de conceptos tales como recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos, el presente trabajo dará a conocer y a verificar las seguridad informática que existe en los procesos internos de una compañía donde se asegura la implantación de sistemas informáticos donde se verifica la información más relevante de las entidades o organismos que existen en Colombia ,nos basaremos en la investigación de los principales incidentes que existe en los equipos de red team y blue team teniendo como base la normatividad que existe en Colombia, quien es el encargado de estandarizar las normativa de la información, como referencia a la seguridad informática.

Este trabajo recopila la información del estudio de la seguridad informática en la gestión de calidad de la información, como también la implementación de la misma en el respaldo y en la arquitectura del equipó red team y blue team con énfasis en los procedimientos de validaciones y contención de vulnerabilidades y respaldos de la información de las entidades que existen en Colombia, refiriéndose a los distintos temas que comprenden el entorno informático que está regida por la constitución política de Colombia que contiene para su desarrollo en el mundo, por lo que este trabajo ayudara a despejar las distintas dudas o inquietudes que a través de la normatividad informática se ha planteado para su estudio en cualquier entorno donde se emplea las diversas condiciones.

A su vez, este proyecto le brinda un gran beneficio para que requiera conocimientos acerca de seguridad informática, como guía para su posterior ejecución, también en definiciones y conceptos básicos de los riegos de informáticos con la utilización y la validación de los equipos blue team y red team.

OBJETIVOS

2.1 OBJETIVO GENERAL

Por medio de unas interrogantes dar a conocer la importancia de un análisis de riegos informáticos para una empresa o para el sector público, teniendo en cuenta su alcance en la vida cotidiana.

2.2 OBJETIVOS ESPECÍFICOS

Establecer los parámetros en el cual se implementa un sistema de análisis de riegos dentro de una organización teniendo en cuenta los conceptos básicos que se emplean para salvaguardar la información.

Dar a conocer las prácticas del análisis de riegos ante una incidencia de seguridad informática tenido en cuenta su alcance en diversas áreas.

DESARROLLO DEL INFORME

Análisis de la legislación relacionada con delitos informáticos dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Se establece para los sectores privados se rige por una normatividad del manejo de la información, teniendo como ejemplo el estudio riguroso de la seguridad informática en Colombia, se estableció en la normatividad del manejo de la información para instituciones establecidas en Colombia, aspectos relevantes como la privacidad de la información de los aplicativos de la empresa o de la institución por eso se establece de la siguiente manera “La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes tomado de la constitución política de Colombia 1991, ley 1273 del año 2009”.

Teniendo en base lo anterior del nivel del respaldo de cloud a nivel nacional el impacto estará referenciado a la capacidad de los servicios solicitados por tal manera se plantea la problemática de los servicios cloud en Colombia el impacto de los servicios cloud en los últimos años se ha convertido como un nivel de respaldo de 75% con referente al sistemas obsoletos , se evidencia que ataques a estos sistemas de seguridad un aumentado tenido como problemática los niveles de servicios establecidos en Colombia como a su vez el desconocimiento de los alcances de estos servicios a instituciones privadas o publicas

Estos servicios en su totalidad están regidos por clausulas y normas que se establecen durante el contrato de servicio, pero en su gran mayoría cuando se adquiere los servicios se desconocen su protección cibernética como también su respaldo en caso de falla de servicio.

Se establece para los sectores privados una normatividad del manejo de la información, teniendo como ejemplo el estudio riguroso de la seguridad informática en Colombia, se estableció en la normatividad del manejo de la información para instituciones establecidas en Colombia, aspectos relevantes como la privacidad de la información de los aplicativos de la empresa o de la institución por eso se establece de la siguiente manera “La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes tomado de la constitución política de Colombia 1991 , ley 1273 del año 2009”.

Tomando como referencia esta política establecida en la constitución política de Colombia es claro que los operadores de servicio s de internet o de servicios de cloud, tienen como base la reglamentación establecida da en la política colombiana de la protección de los datos de sus clientes, así como también el respaldo de la información.

Durante los servicios prestados en Colombia se establece que el manejo normativo de la información de los diferentes procesos del almacenamiento de datos está regido por la siguiente normativa en la constitución política de Colombia, observando que “Ley 962 de 2005 Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de ló el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados” tomado de la constitución política de Colombia 1991, ley 1273 del año 2009

Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales establece la protección personal de la información almacenada en medios magnéticos como también en infraestructuras cloud acompañadas por un contrato de vigencia donde ese aclara el servicio y sus s alcance estableciendo un modelo de protección de la información

Durante los servicios prestados en Colombia se establece que el manejo normativo de la información de los diferentes procesos del almacenamiento de datos está regido por la siguiente normativa en la constitución política de Colombia, observando que [1]“*Ley 962 de 2005 Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de ló el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados*”

[1] Ley 962 de 2005 - Gestor Normativo. (s/f). Gov.co. Recuperado el 14 de noviembre de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=17004

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting, usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición a incorporar un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Las pruebas de seguridad informática por el método de pentesting relaciona las vulnerabilidades de los sistemas de información teniendo en cuenta la referencia tecnológica en el cual se ha validado, don la información más sensible o especifica se le realizara varios procedimientos donde se validara la infraestructura y la arquitectura del software en donde está almacenado la información , teniendo como objetivo la relación de la seguridad informática en los procesos alternos de las políticas de acceso a la información.

Dentro de la simulación donde un atacante utiliza varios intentos de penetración ala nivel de software y de conexión digital, se evidencias los fallos más comunes en el proceso de consulta de la información dentro de un sistema informático, es válido a clara que para los sistemas de información hay normativas que ayudan a la protección de la información ante estos ataques por lo cual pentesting ayuda a la validación de estos sistemas de información a ser más protegidos.

Dentro de este análisis existen pruebas de infiltración a la base de datos, que concite por medio de un ataque específico por comandos de consulta de MySQL la validación de la información que existe en los sistemas informáticos, estructuralmente están protegidos por medio de código de programación donde encripta las consultas, pero en ocasiones no se configura correctamente el cual queda sin protección es fácil la validación directa en la base de datos.

Para el análisis de la información dentro de los servidores se valida su infraestructura en sus conexiones donde se valida la conexión primaria es decir la conexión física de no haber vulnerabilidades se realiza un ataque donde los comandos de conexión y de respuesta se realiza la conexión por comando al router de la conexión LAN.

Para estas pruebas se dividen en los siguientes parámetros donde los ataques son caracterizados por su tipo de penetración y de finalidad, donde evidencia que para las compañías es fundamental validar las políticas de la información y de registro de la información donde se evidencia los ataque es más específicos ala la información más sensible de la compañía.

Pruebas orientadas a un objetivo

Para estas pruebas se valida su finalidad es decir determinar su objetivo principal por lo cual es establecido una ruta específica para obtener la información o validar los parámetros de conexión, donde se utiliza un medio de penetración al sistema de información y en ocasiones valida también el tratamiento de la información en los diversos procesos de las compañías.

Comprobación externa

Están relacionado para los sistemas de red de conexión y de envió de información ejemplos la configuración deservidores de correo de conexiones a red de internet y conexiones a equipos remotos donde se valida sus puertos de conexión y de validaciones de límite de conexiones donde se evidencia las deficiencias de las configuraciones de red y de privacidad de la información.

Pruebas internas

Se empela una conexión dentro de la empresa empleado los privilegios de los administradores de sistema donde se relación a la configuración de usuarios de dominio y también de autenticación a la red en ocasiones estos ataques simulados detectan que no hay protocolos de autenticación de registro entre usuarios y también una manipulación indebida del firewall.

Pruebas a ciegas

Esta prueba relaciona los ataques a las compañías donde se hace un ataque real con sistemas de ataques variados para obtener vulnerabilidades estas pruebas llevan demasiado tiempo ya que se utiliza varios ataques de penetración de código por fuerza bruta donde se realiza las especificaciones a largo plazo este ataque es específico para compañías ya que es un taque simado muy costo.

Pruebas de doble ciego

Se realiza la combinación de la fuerza ciega y la infiltración de una gente de seguridad informática donde se valida las medidas y el respaldo de información cuando hay un ataque real para obtener como objetivo mejorar la seguridad informática, solo empresa especialista en seguridad informática son capaces de realizar los reportes de seguridad a la información sistemáticamente.

Pasos de pentesting Recopilación de información

Como primera medida de implementación de pesting está la recopilación básica de la estructura de la información para adecuar el procedimiento del ataque con la validación de la gerencia tecnológica de la compañía u organización, ya que esta información preliminar destacaría toda la trazabilidad de la información Análisis de vulnerabilidades por medio de herramienta de escaneaos de primer nivel si haber ataque preliminares el objetivo es recopilar la información y establecer el objetivo del ataque teniendo ene cuneta los parámetros básicos de la información almacenadas en los sistemas de información.

- Nmap
- Dnsmap
- Dnsrecon
- Recon-ng
- SubFinder

Análisis de información

De pues la recopilación de la información se valida cual es el mejor método de infiltración al sistema informático teniendo en cuenta la trazabilidad final de la información y su almacenaje para esta operación se identifica las posibles rutas y los sistemas de infiltración el cual se procede con el test de vulnerabilidades con la configuración de seguridad de primer nivel como lo es la negligencia en la configuración de puertos de conexión en los sistemas informáticos como lo son.

- Configuración de seguridad defectuosa
- Componentes vulnerables y obsoletos
- Fallos de identificación y autenticación
- Fallos en el software y en la integridad de los datos
- Fallos en el registro y la supervisión de la seguridad
- Falsificación de Solicitud del Lado del Servidor

Análisis de información

De pues la recopilación de la información se valida cual es el mejor método de infiltración al sistema informático teniendo en cuenta la trazabilidad final de la información y su almacenaje para esta operación se identifica las posibles rutas y los sistemas de infiltración el cual se procede con el test de vulnerabilidades con la configuración de seguridad de primer nivel como lo es la negligencia en la configuración de puertos de conexión en los sistemas informáticos como las siguientes configuración.

- Configuración de seguridad defectuosa Componentes vulnerables y obsoletos Fallos de identificación y autenticación

- Fallos en el software y en la integridad de los datos Fallos en el registro y la supervisión de la seguridad Falsificación de Solicitud del Lado del Servidor

Algunas de las herramientas más usadas en esta fase son las siguientes:

- Nessus
- OWASP
- Zap Proxy BugBounty
- Recon
- Vega
- BurpSuite

En esta etapa los resultados son significativos dentro del proceso por lo cual se establece varias características de infiltración del ataque teniendo en cuenta características de conexión modo de almacenamiento y validación del estado de la red interna o de los sistemas activos de información.

Explotación

La explotación esta referenciado por la utilización de herramientas de ética hacking donde se realizar la infiltración a los sistemas de seguridad de los sistemas de información tal es la validación del código fuente en donde se realiza la validación de los sistemas informáticos teniendo en cuenta la relación de la estructura de seguridad como ejemplo se realiza la validación de seguridad en cuanto a la conexión de la base de datos y seguridad informática.

los objetivos de la explotación del ataque simulados son:

- Información confidencial
- Validar los protocolos de seguridad informática
- Almacenamiento de la información
- Clasificación de la información
- Stock de sistemas de información
- Acceso a información sensible
- Validación de las debilidades de los sistemas informáticos
- Inventario y arquitectura de la red interna de información

Los resultados podrían variar dependiendo del tipo de ataque ya que haya algunos que tardan mas tiempo en la explotación y en la adquisición de los resultados, obteniendo que los sistemas de seguridad de los sistemas de información son revisados en los protocolos de obtención y de transmisión de los datos.

Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético

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

Teniendo en cuenta que la empresa es una empresa de seguridad informática por lo cual tiene como responsabilidad regir su procedimiento con la legalidad de su país, no es aceptable de ninguna manera que al receptor de la información lo obliguen a no divulgar procedimientos de carácter malintencionado que está prohibido por la ley ya que los actos ilegales pueden afectar directa o indirectamente a terceros.

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

Se obliga directamente al recepto no divulgar chuzadas o intercepciones ilegales que pude hacer la empresa, teniendo en cuenta esta irregularidad, esta cláusula o definición de contrato no es legal ya que los términos de chuzadas y interceptación e al información son delitos y solo organismos autorizados por el estado son los que podrían hacer estas acciones, teniendo en cuenta los siguientes leyes establecidas para la protección e al información [2]"*Ley de Protección de Datos Personales o Ley 1581 de 2012 Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las*

2Política de Protección de Datos Personales. (2021, agosto 4). Ministerio de Ambiente y Desarrollo Sostenible. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. " y la ley de protección de la información en sistemas de información [3]"*Ley 1273 de 5 de enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Diario Oficial nº 47.223)."*

Cuarta. Responder por el mal uso que le den sus representantes a la información confidencial y Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

En esta cláusula se evidencia que tienen una reglamentación poco ética ya que el firmante dispone su responsabilidad ante delitos informáticos y de ser hallada la empresa el estaría como directo responsable de la información de terceros que se estén manejando de manera inadecuada en la compañía, por lo cual

esta cláusula obliga claramente a liberar de cualquier responsabilidad de la empresa teniendo como objetivo hacer responsable al empleado o al usuario firmante.

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

Con relación a la cláusula cuarte en la característica 3 , es irregular y poco ético que se obligue a no divulgar acerca de los delitos que están haciendo la empresa a las autoridades competentes , ya que de ser hallados culpables de algún delito informático el usuario o receptor firmante estaría asociado al delito por omisión sin importar la ley interna de la empresa ya que primeriza las leyes colombianas ante los delitos informáticos y los delitos contra la integridad de terceros según los establecido en la ley [4]"*Código Civil Artículo 1519. Objeto ilícito Hay un objeto ilícito en todo lo que contraviene al derecho público de la nación. Así, la promesa de someterse en la república a una jurisdicción no reconocida por las leyes de ella es nula por el vicio del objeto*"

Cuarta. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas y en la parte novena La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.

[3] Cuervo, J. (2009, julio 29). Ley 1341 Principios y conceptos sobre la sociedad de la información - Informática Jurídica. Informática Jurídica. https://www.informatica-juridica.com/ley/ley-1341-principios-conceptos-la-sociedad-la-informacion/

4 Código Civil Artículo 1519. Objeto ilicito. (s/f). Leyes.co. Recuperado el 14 de noviembre de 2023, de https://leyes.co/codigo_civil/1519.htm

Según las características anteriores al firmante se le obliga ano divulgar los delitos que en la compañía incurra esto es poco ético ya que como ciudadanos estamos obligados a denunciar cualquier procedimiento ilegal sobre la información o el actuar de algunas compañías teniendo en cuenta que ellas se rigen por estatutos legales como nos dicen la siguiente ley [5]"*Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos*"

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora 1. Mantener la reserva de la información confidencial hasta tanto

No se estipula la relación de fechas ni condiciones finales de la reserva de información asegurándose a la empresa de modificaciones o controversias por no estipular tiempos de divulgación.

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

Teniendo en cuenta esta cláusula el firmante del contrato se hace responsable por vía legales de resolver cualquier divulgación de procedimientos ilegales , violando cualquier libertad de defenderse del firmante ante un delito informático , validando también que la empresa no tiene ética laboral y dispone solos de intrusiones de confidencialidad donde se aclara que cualquier inconsistencia el fírmate se hace responsable de su solución en cualquier caso [6]"*Ley 1341 de 30 de julio de 2009, sobre principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones (Diario Oficial nº 47426 de 30 de julio de 2009). (Deroga el Artículo 51 de la Ley 1978 de 25 de julio de 2019 el Artículo 66 de la Ley 1341 de 2009).(Declarada exequible por la Sentencia C-127 de 2020 de la Corte Constitucional*)."

[5] Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s/f). Senado de la Rep□blica de Colombia. Recuperado el 14 de noviembre de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[6] Cuervo, J. (2009, julio 29). Ley 1341 Principios y conceptos sobre la sociedad de la información - Informática Jurídica. Informática Jurídica. https://www.informatica-juridica.com/ley/ley-1341-principios-conceptos-la-sociedad-la-informacion

Análisis de los anexos, en relación con la vulneración de la ley 1273 argumentando cualquier proceso ilegal.

Teniendo en cuenta el análisis de la legalidad del contrato se encontraron los siguientes aspectos que violan la ley de protección de la información protección de la información y de los datos estipulada en la ley 1273.

[7]Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

Por lo cual está estipulado en la ley que sin estar capacitado ejecuta esta acción de compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique información sensible por lo cual en los parámetros del contrato estaría incurriendo contantemente en la complicidad de la empresa en sustraer información ilegalmente en su plena ejecución de sus funciones referenciados en los siguientes puntos.
Segunda. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

[8]Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO

En donde se aclara que cualquier interceptación de información o sustracción ilegal no autorizada es motivo del delito tenido en cuent6a esto en el contrato le obliga al firmante que cualquier delito informático de sustraer información curde confidencialidad la empresa y el directamente sería el responsable en los siguientes parámetros del contrato a definer

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora 1. Mantener la reserva de la información confidencial hasta tanto

Cuarta. Responder por el mal uso que le den sus representantes a la información confidencial y Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento

[9]ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFOMÁTICOS.

Las chuzadas en la cuales la ley de protección a la información estaría totalmente prohibida y solo autoridades legales lo pueden disponer, pero en el caso de empresas no están autorizadas y estarían incumpliendo en la reglamentación d legal de la información según ene contrato en el párrafo segundo.
Segunda. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad,

[7] Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_0599_2000_PR007]. (s/f). Senado de la República de Colombia. Recuperado el 14 de noviembre de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr007.html

[8] Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s/f). Senado de la República de Colombia. Recuperado el 14 de noviembre de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

9 Normatividad sobre delitos informáticos. (2017, julio 25). Policía Nacional de Colombia. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

Es importante resaltar las políticas de seguridad que hoy en día están implementadas en América latina y el caribe, para velar por la información privada de las empresas y organismos institucionales de los diferentes países que la conforma, teniendo como principal objetivo el derecho a la privacidad y la protección de datos sensibles, teniendo como principal objetivo el tratamiento de la información de los ciudadanos que utilizan los sistemas de información para facilitar procesos de vital importancia.

Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.

Teniendo en cuenta el análisis de las características del contrato no sería viable el aceptar el contrato ya que por ética laboral de ingenieros estaría actuando como un cómplice de la ilegalidad atentando a terceros e incurriendo en graves delitos, adicional validando toda la legalidad que rige la distribución colombiana nos indica que esta situación no es favorable, ya que al ser cómplice de un delito informático las penas irían entre 8 a 48 años de prisión sin tener en cuenta la caución monetaria que me traería incurrir en los delitos informáticos,
por lo cual la empresa se exonera de cualquier responsabilidad al momento de afrontar la responsabilidad de los delitos informáticos esto sería poco ético por parte de la compañía WhiteHouse Security, ya que la ética de los ingenieros según la estructura que legaliza y acredita nuestra funciones nos dice que estamos en la obligación de denunciar toda actividad ilegal al en el cargo de nuestras funciones y que de haber un caso relacionando perderíamos nuestra certificación como ingeniero s don estaríamos reportados por tal incidente, adicional se han evidenciado casos donde la reputación de funcionarios de la información se a perdido por ganarse un monto especifico de dinero nosotros somos profesionales y ningún monto de dinero por ser muy alta no omitiría nuestra educaciones y ética laboral , teniendo ene cuenta nuestro trayecto como ingenieros de sistemas en una compañía de dudosa reputación , ya que estos eventos son muy comunes y estamos expuestos a chantajes y ofrecimientos de negocios ilícitos en nuestra labor diaria como administradores de información de una compañía, adicional las empresas establecen que cada día haya cada vez más seguridad de la manipulación y divulgación de la información por lo cual las empresas se están capacitando y certificando para la seguridad informática por lo cual están teniendo tendencias de seguridad guardando los pilares de información, que es integridad, disponibilidad, confidencialidad ya que en estos pilares se realiza la gestión ordenada y adecuada de la manipulación de datos de una persona o empresa en las organizaciones tiene como obligación capacitar y tener un departamento que vigile cualquier irregularidad que pase con los datos de los clientes como los datos de las personas que tenga un fin especifico tal es el caso de que bloqueos y contratos como cláusulas de confidencialidad están sujetos a disposiciones de la empresa con validación de los usuarios, características que tienen como objetivo la protección de un sistema de información es así que se tienen un campo dentro de la informática especializada en implementar políticas que protegen la integridad de la información dentro de un sistema informático , teniendo en cuenta que cada día hay nuevas tendencias tecnológicas que no afianza con la seguridad ya que es de vital importancia la integridad de un sistema informático.

Todo esto estipulado en el siguiente párrafo de la ética de COPNIA [10]"*PARÁGRAFO. El Código de Ética Profesional adoptado mediante la presente ley será el marco del comportamiento profesional del ingeniero en general, de sus profesionales afines y de sus profesionales auxiliares y su violación será sancionada mediante el procedimiento establecido en el presente título*"

Lo anterior se establece que en plana actividad de nuestra función es de precisar que para muchos de nuestro caso de recepción y tratamiento de información nuestra ética

[10] El Código de Ética (S/f). Gov.co. Recuperado el 14 de noviembre de 2023, de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

laboral está presente por lo cual cualquier responsabilidad ilegal está ligada en nuestra profesión es preciso aclarar que estamos sujetos al manejo de cualquier dato almacenado y que esta información en muchas de la ocasión es de carácter privado y de esa información depende nuestra reputación en ser dispuesta nuestra amanera de ser profesionales en nuestra área.

Análisis del caso "OPERACIÓN ANDROMEDA BUGGLY"desde su posición teniendo en cuenta los aspectos legales y éticos.

Realizando una análisis de la operación de descubrimiento del ciber ataque ilegal sobre los diálogos de paz (**OPERACIÓN ANDROMEDA BUGGLY**), hay que hacer un concepto de la definición sobre que es una chuzada, esta es una forma de interceptar información por un medio ilegal y sustraer la información más sensible para fines no legales , estas interceptaciones en Colombia las majean con anterioridad el DAS, teniendo como objetivo primordial la captura de criminales, esta interceptaciones utilizaban herramientas de interceptación telefónicas que iban de sistemas físicos con instrumentos especializados de conexión ilegal para la telefonía fija, hasta la interceptación de la telefonía móvil, que ya se realizaba con medios tecnológicos avanzados y solicitando la autorización por medio de canales de comunicación fiables y con la autorización del operador quien manejaba el servicio, a raíz de de escándalos de interceptaciones (chuzadas), no autorizadas y con fines no especificados el DAS, cerro sus operaciones, por lo cual ningún organismo del estado puede realizar estas interceptaciones, esta reglamentaciones esta reforzada en la constitución política de Colombia en la siguiente Código Penal Artículo 196 Colombia

[11]"*artículos 192 y 193 del Código Penal, los cuales establecen los delitos de violación ilícita de comunicaciones y de ofrecimiento, venta o compra de instrumentos aptos para interceptar comunicaciones privadas*", estas interceptaciones están clasificada como delitos, en el ámbito tecnológico también existen la chuzadas como medio de sustracción ilegal de información de terceros para fines criminales, por lo cual en el famosos caso Andrómeda existió unos aspectos a resaltar ya que se revelo a través de la prensa el objetivo por el cual se había n realizado las interceptaciones y se conoce adicional su modo operativo de sustracción de información.

Definición de aspectos más relevantes

- Su confirmación es la siguiente como primera medida en el ámbito de infraestructuras se conoce que los equipos de cómputo eran aportados por una firma de publicitas para la campaña de Oscar iban Zuluaga, que un principio era para la publicidad de la campaña, por lo cual eran equipos con tecnología de gama media a alta , dirigido por un servidor y un servicio especial de internet de 24 horas de ancho de banda de más de 50 megas tenía como objetivo disimular las intenciones del lugar ya que en el primer piso se ubicaba un restaurante y en el segundo se ubicaba aparentemente un café internet con video jugadores para lo cual en ese tiempo era muy recurrente estos lugares donde los video jugadores se reunían sin levantar sospecha alguna.

11.Constitución Política De Colombia. (s/f). Justia.com. Recuperado el 14 de noviembre de 2023, de https://colombia.justia.com/nacionales/constitucion-politica-de-colombia/titulo-vii/capitulo-1/

- Su organización estaba basada por un ingeniero hacker, comandando a otros para sustracción de información, este ingeniero con mayor conocimiento diría y

  comandaban a los demás integrantes para utilización de información dentro de la fachada de buggly.

- Su modo opérandi era el siguiente a través de un programa de navegación y una herramienta de análisis de tráfico y la utilización de código de desencriptación de correos obtuvieron acceso a un correo especifico donde tenían una lista especifica de correos, donde se enviaban información de los diálogos de paz de ese año, teniendo como base primordial saber que temas estarían tratando y que opiniones salían para ser utilizados de manera arbitraria para las elecciones del mismo año

- Conocimiento la información del uso del lugar para interceptaciones se filtró la información por lo cual se confirmó que algunos militares estaban en relación con las interceptaciones y el conocimiento de la información sustraída para dudosos beneficios.

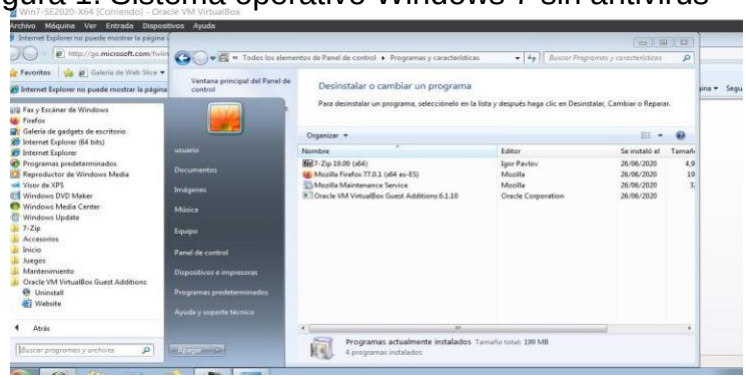
Teniendo en cuenta esas características se concluye que la ética profesional y la información en la cual nosotros estamos involucrados no es para ser utilizada para fines políticos en el cual se evidencia que los actores de este caso tenían firmes convicciones de utilizar la información para fines privados, por lo cuales los medios tecnológicos y los conocimientos tecnológicos están sujetos a delitos informáticos , por lo que al final fueron descubiertos y estas personas están inmersos en un delito informático que se emplea diversas herramientas de haking donde sustrajeron la información lo mas resaltante es que este conocimiento no es empírico si no que fueron adquiridos por un hacker avanzado en temas tecnológicos teniendo como objetivo adquirir medios de sustraer información atreves de un grupo de hackers, nuestra profesión estamos inmersos en diversos emdiod e divulgación de información depende de nosotros y nuestra ética laboral si optamos por cometer un delito informático ya sea por un medio digital para fines, donde mancharía nuestra hoja de vida profesional ante un presunto delito ilegal.

Analizando el caso se valida que en el sistema operativo hay ciertas inconsistencias en su configuración de puertos de seguridad por lo cual se procede con el análisis de puertos por medio de la herramienta de seguridad de Kali Linux según pasos de un pentesting.

Reconocimiento

En este paso identificamos los actores del caso el computador inicial tiene sistema operativo Windows 7 con baso de sistema operativo a los x64, teniendo en cuenta se validara si tiene instalado una aplicación que genero la fuga de los datos, por lo cual se analizar inicialmente que seguridad tiene el equipo por lo cual se identifica que no existe un antivirus y el firewall esta activado, por lo cual se analizara internamente con un programa especial en la trasmisión de información a través de la red LAN.

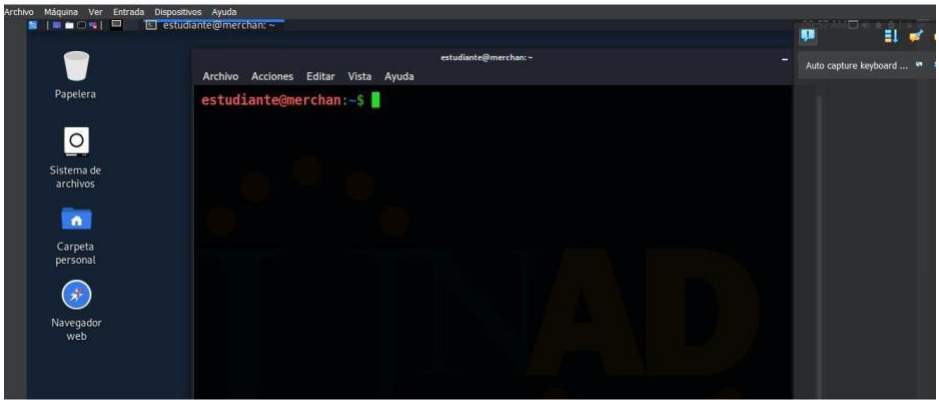
Figura 1. Sistema operativo Windows 7 sin antivirus



Fuente: Elaboración propia

Con un programa de análisis de vulnerabilidad se procede bajo comandos de conexiones de red y de análisis de trafico la detención del software que está generando la incidencia ya que se a detectado d que directamente no hay programas instalados que se evidencien como malware en el equipo.

Figura 2. Programa de análisis de vulnerabilidad Kali Linux

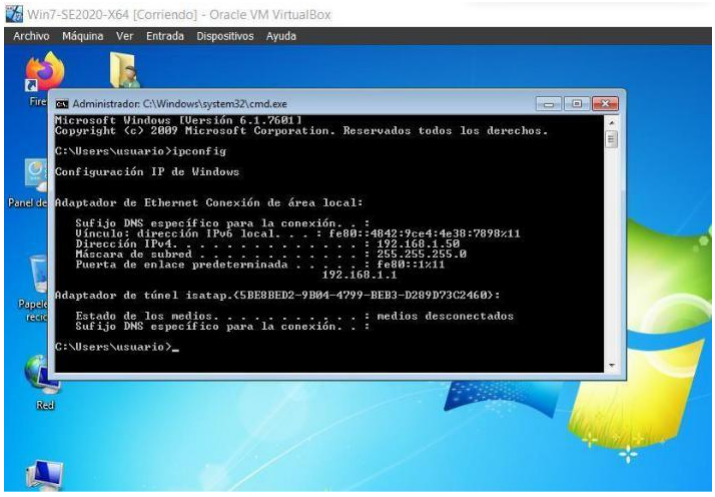


Fuente: Elaboración propia

Análisis de vulnerabilidad

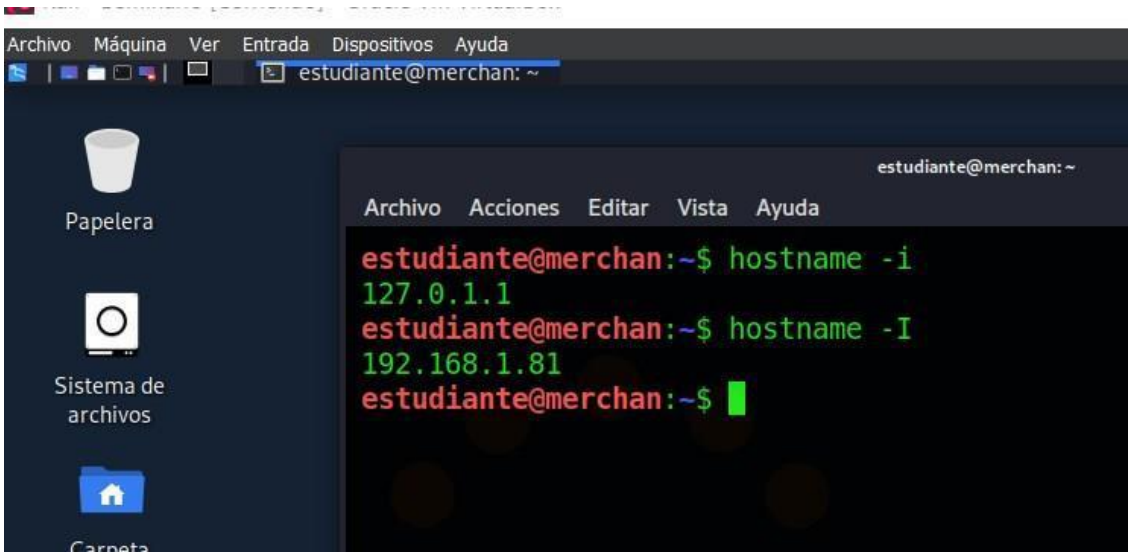
Se procede un análisis de red con la herramienta de Kali Linux de Nmap que valida los puertos de conexión de la red con referencia de los equipos donde encontramos que hay un puerto que este habilitado que lo maneja una aplicación desconocida de la aplicaciones y comandos de Microsoft

Figura 3.IP de Windows x64



Fuente: Elaboración propia

Validamos la ip de la maquina con Windows 7 x64 Figura 4.Ip de Kali Linux

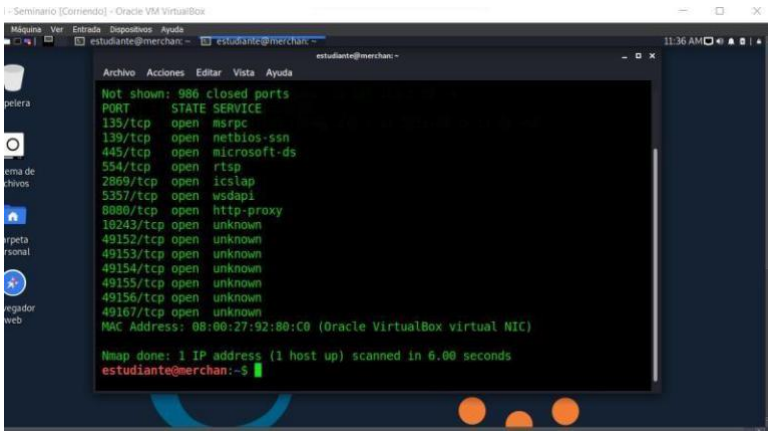


Fuente: Elaboración propia

Ip de la herramienta software de análisis de vulnerabilidades Kali Linux

Anualizamos los puertos conectados través del comando interno en la consola de Kali Linux nmap sudo nmap -Ss 192.168.1.50 -A con privilegios de Kali y detectamos con el comando versión de sistema operativo y lo puertos habilitados, encontrado que hay un puerto inseguro el cual es 8080, validamos con la ip el puerto y que clase de programa está instalado desde otro equipo.

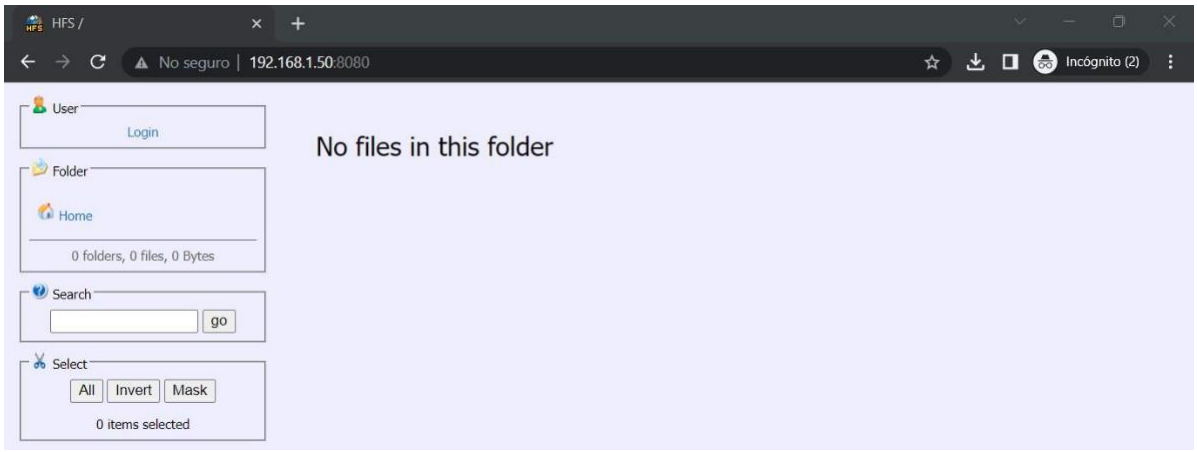
Figura 5. Puertos de conexión Kali



Fuente: Elaboración propia

Se valida que el puerto 8080 está abierto para conexiones y hay un servicio http-proxy de conexión a aplicaciones web.

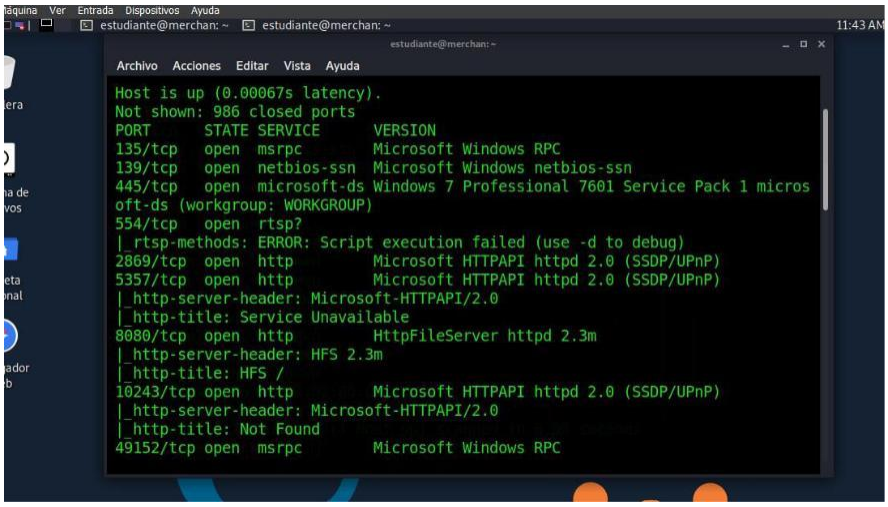
Figura 6. programa remoto de archivos



Fuente: Elaboración propia

Se valida por medio del navegador web que aplicación está emitiéndose a través de ese puerto de conexión sin autorización del usuario el cual es una aplicación de web se servicios remotos.

Figura 7. comando de verificación de puertos

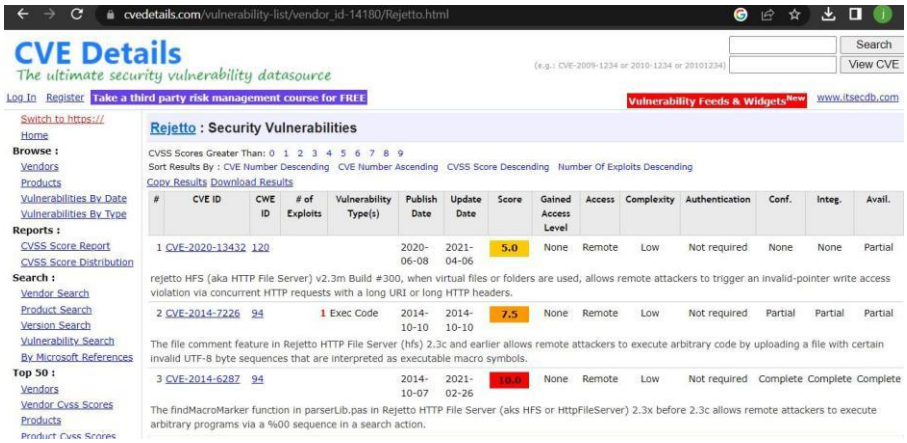


Fuente: Elaboración propia

Se valida a profundidad especificaciones del servicio encontrando el servicio de transferencia de archivos host de servidor local HF con la versión 2.3m.

Analizando el puerto de conexión 8080 identificamos que tiene un servicio http server don se identifica que está habilitado el servicio de conexión al puerto de conexión 8080 por el programa de conexión remota Remote Command Execution rejetto v. 2.3 donde esta vulnerabilidad es de nivel media alta para crear archivos y transferir a través de puerto de conexión sin habilitado por el firewall de Windows.

Figura 8. validación vulneración rejetto



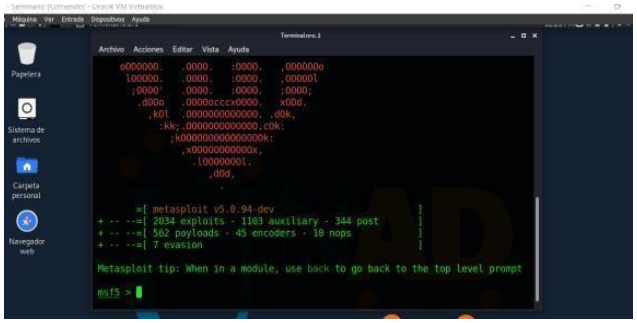
Fuente: Rejetto : Security vulnerabilities, CVEs. (s/f). Cvedetails.com. Recuperado el 14 de noviembre de 2023, de https://www.cvedetails.com/vulnerability-list/vendor_id-14180/Rejetto.html

por medio de control remoto se evidencia que puede crear usuarios modificación de archivos trasferencia de archivos ya que la aplicación se ejecuta en un segundo plano y sin autorización del usuario pueden realizar varias configuraciones.

Escalamiento De Privilegios

por medio de la aplicación metasploit framework de Kali se procede con la asignación de un usuario administrador

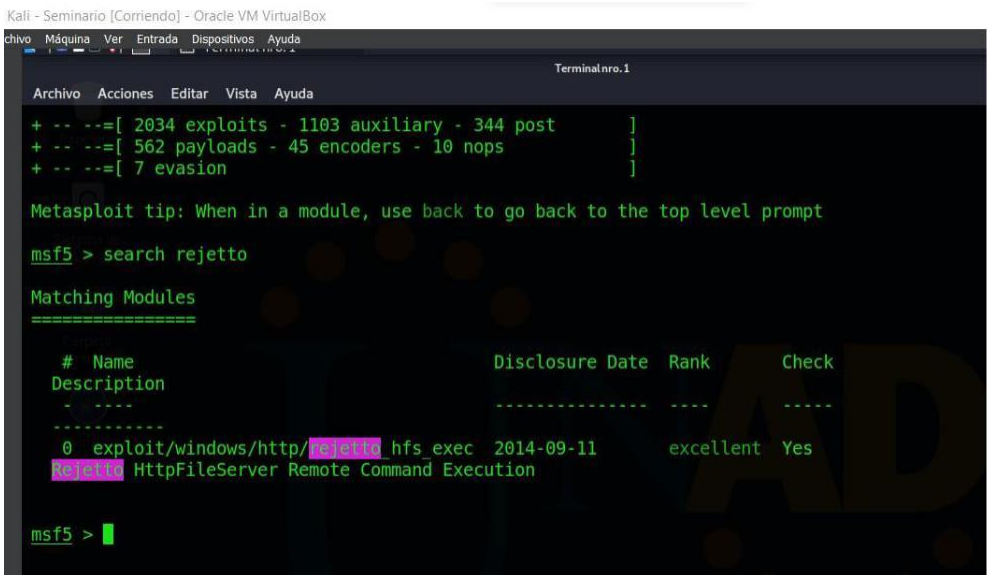
Figura 9. metasploit framework



Fuente: Elaboración propia

Abrimos la aplicación metasploit framework donde escaneamos la victima para crear un archivo script a la maquina y obtener parámetros con privilegios administrativos por medio de comandos.

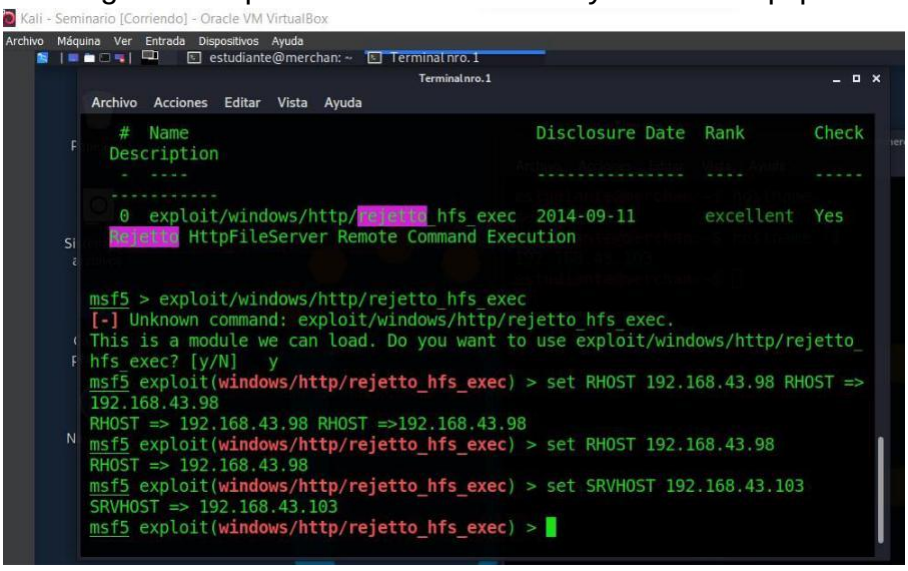
Figura 10. comando de exploit rejetto



Fuente: Elaboración propia

Buscamos a través del comando search rejetto para validar dentro de nuestra red cual es el equipo que tiene ese servicio, ya que la aplicación nos da esa información a través de otro comando de búsqueda y de conexión por medio de comandos.

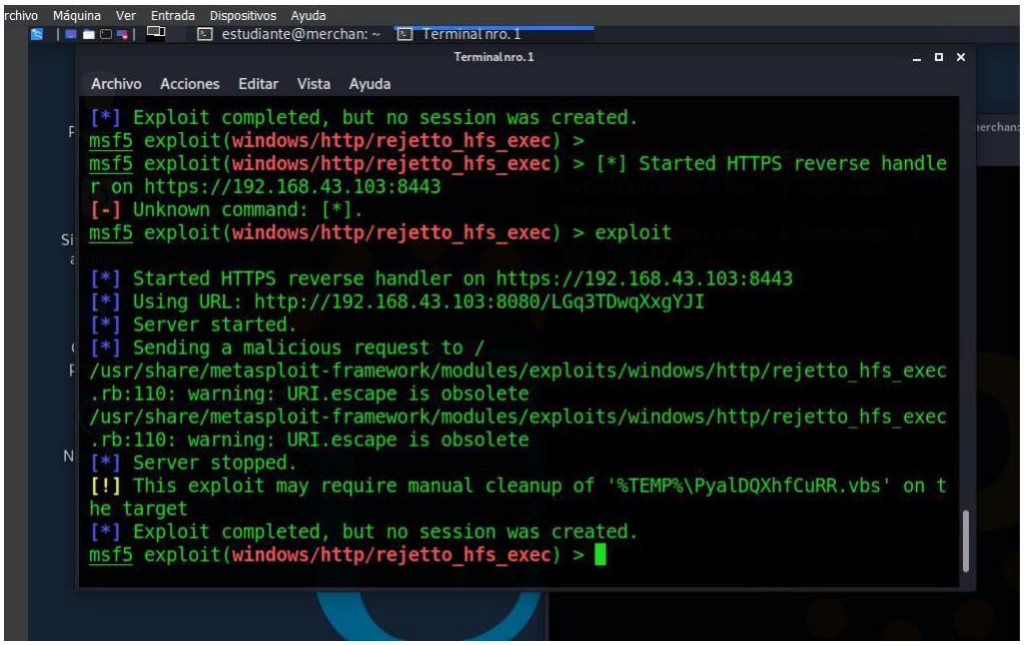
Figura 11. aplicación comando de inyección al equipo de la victima



Fuente: Elaboración propia

Se procede con la asignación de ip de la máquina de atacante y de la víctima a través de los comandos de SET RHOST para la víctima y para el atacante SET SRVHOST.

Figura 12.Envio de script a la victima traes de host



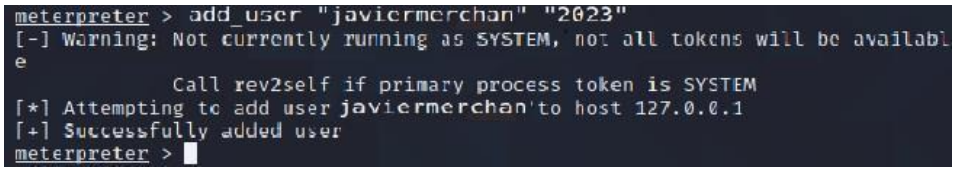
Fuente: Elaboración propia

Se envía a través de conexión del exploit el scribt malicioso a través de la aplicación rejetto

Figura 13. validación creación de usuario

Fuente: Elaboración propia

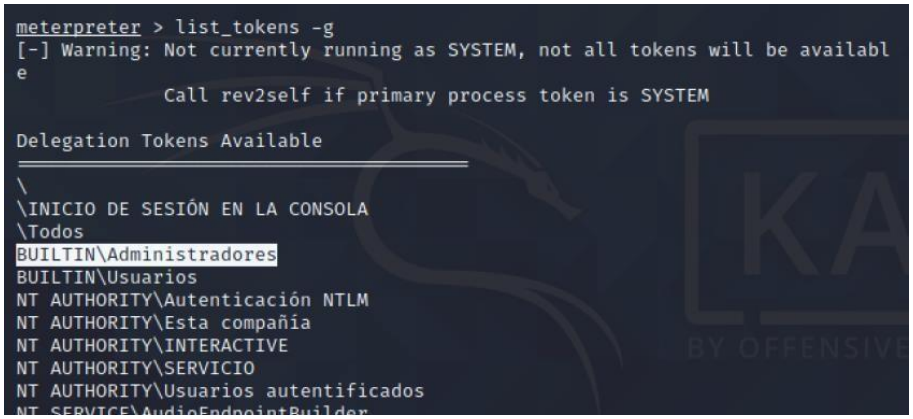
Figura 14. comando meterpreter creación usuario



Fuente: Elaboración propia

Por medio del comando de inserción meterpreter se procede con la asignación del nombre del nuevo usuario y de asignación de permisos

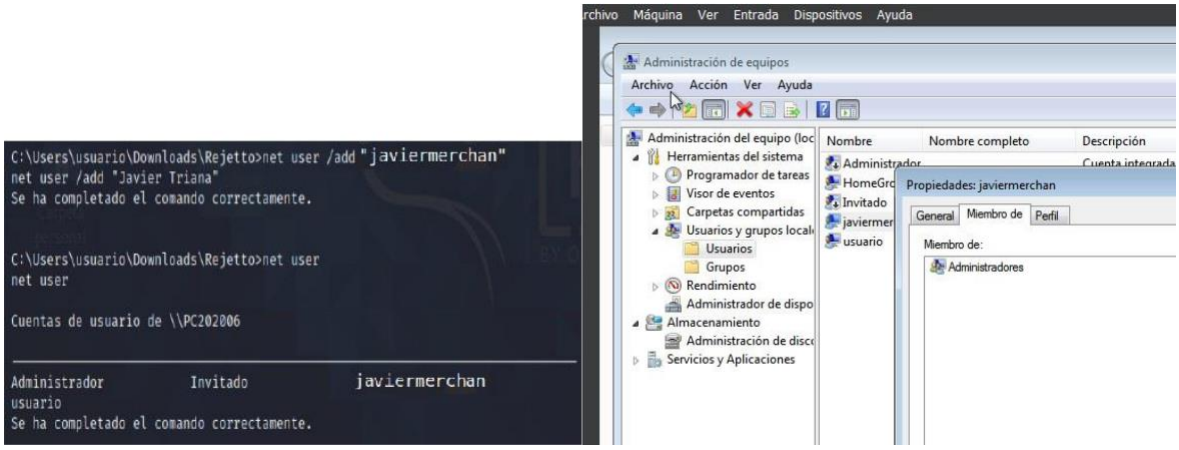
Figura 15. listar los permisos



Fuente: Elaboración propia

Se procede con la asignación de permisos de usuario por lo cual se escoge el usuario Javier merchan y se asignan los permisos correspondientes como administrador

Figura 16. comando de verificación de permisos

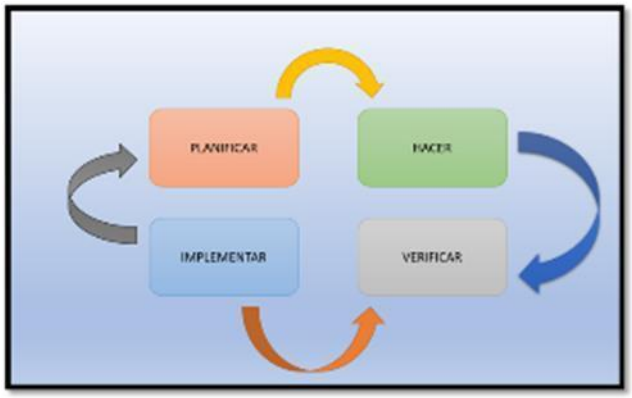


Fuente: Elaboración propia

INFORME DE ANÁLISIS DEL CASO

Teniendo en cuenta el procedimiento llevado por el grupo de equipo ¿Red Team, investigando la seguridad del caso anterior se establece que el nivel de seguridad informática no es el más adecuado por cuanto se establece que la debilidad ene cuando procedimientos en los cuales están referenciados de la siguiente manera?

Figura 17. planificación de gestión de riesgos



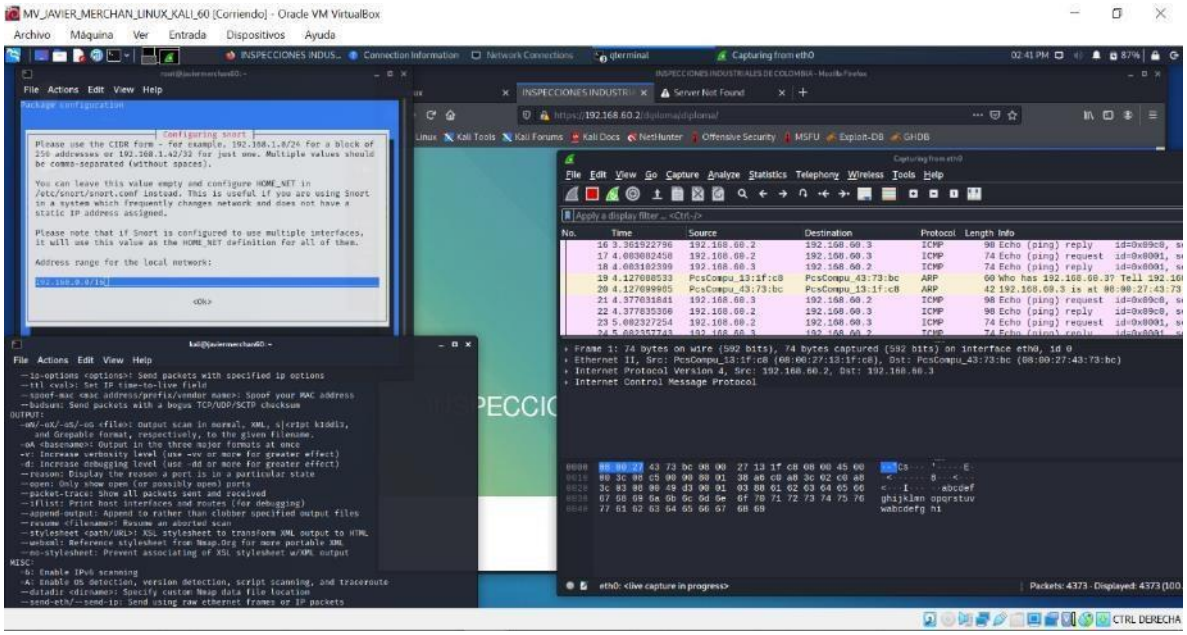
Fuente: Elaboración propia

la arquitectura organizacional de una empresa o de una entidad donde se resalta los procesos administrativos con los procesos tecnológicos, donde se resalta la delegación de funciones donde se estructuran los procesos internos o externos donde se evidencia la jerarquía de responsabilidad, en el cual los principales actores de la gerencia tecnológica establece protocolos de restricción y de control de la información, que más adelante será auditada constantemente , adicional se establece un modelo de organigrama como los es el cobit, que establece los proceso de gestionar los roles adecuadamente para la ejecución de protocolos de medición de procesos donde un proceso que esta delegado no es adecuadamente gestionado produce un mal funcionamiento del sistema de gestión de la información , adicional se establece protocolos de contingencia del cual se establece medidas de ejecución para información vigilada por el director del área.

Por lo cual se implementar gestiones de control de seguridad en los parámetros de seguridad como es el control de antivirus actualizaciones gestión de seguridad interno para que no se repita nuevamente el caso por lo cual los puertos se controlasen y no habrá medios de filtración de la información.

Los cuales se implementa para mejorar la calidad de empresa como también la certificación con los clientes ya que como por ejemplo los bancos tiene empresas que maneja la gestión de la información con contratos exclusivos con empresas certificadas con normas ISO y haya diversos organismos que apoyan la diversidad de la implementación de elementos de infraestructura y de componentes de desarrollo de lenguajes de programación que regulan todo lo referente al control de calidad de la administración de la información

Figura 19. Análisis aplicativo sharhd



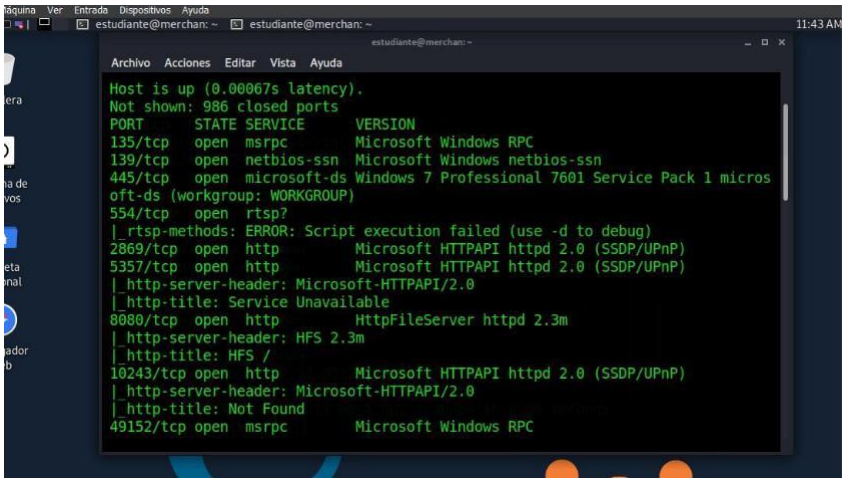
Fuente: Elaboración propia

En informe se valida que este puerto 8080 esta con privilegios y a través del puerto se puede infiltrar o instalar cualquier malware que afecte la información y teniendo en cuenta que está conectado en la red se puede tomar remotamente y tener privilegios de control remoto por lo cual es un peligro para organización con el fin de respaldar la información se debe de formatear el equipo y validar con un buen antivirus todas las conexiones de red en los puertos de conexión de niveles de red.

INFORME CON ANÁLISIS DEL CASO DE RED TEAM, QUE PERMITIÓ DAR SOLUCIÓN AL FALLO IDENTIFICADO.

Inicialmente el equipo de análisis de red team tiene que validar el caso de verificación de los puertos inicialmente se validaron que puertos estaban abiertos adicional el firewall del sistema operativo de la versión 7 a 64 bit validada con el nmapa que contine Kali linux.

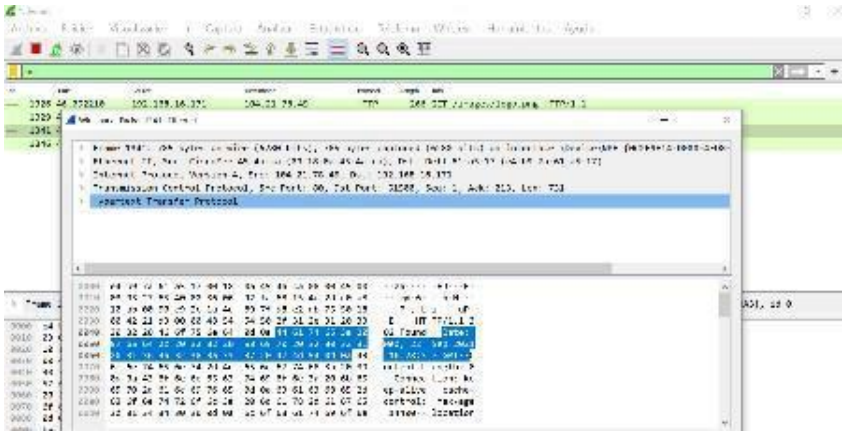
Figura 20. Validación de puerto



Fuente: Elaboración propia

Por lo cual en la validación de todos lo puertos inicialmente se detecta que un puerto de 8080 está abierto y se está ejecutando constantemente, teniendo como consecuencia que no esté autorizado en la verificación del puerto de conexión

Figura 21. Análisis de puertos



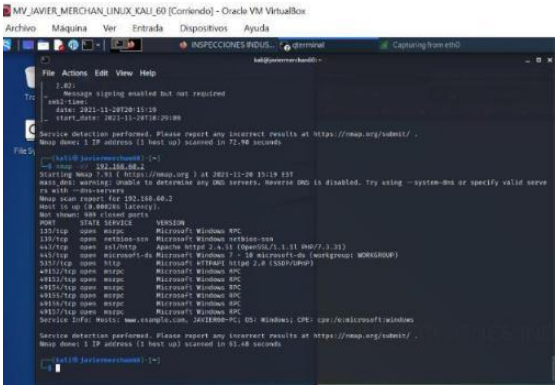
Fuente: Elaboración propia

Como se demuestra en la imagen anterior donde se evidencia el tráfico del puerto 8080 cada vez que se consulta evidenciando que es un peligro para la trasmisión de la información sin ser autorizado.

Informe de herramientas utilizadas para dar identificar fallos en el escenario propuesto.

Para el análisis de la incidencia se validó con el nmapa los puertos de conexión que tenía la ip del computador de la víctima por lo cual este software manda verificaciones en todas las capas de conexión dando como resultado la emisión de puertos abiertos y cerrados.

Figura 22. Análisis de puertos nmap

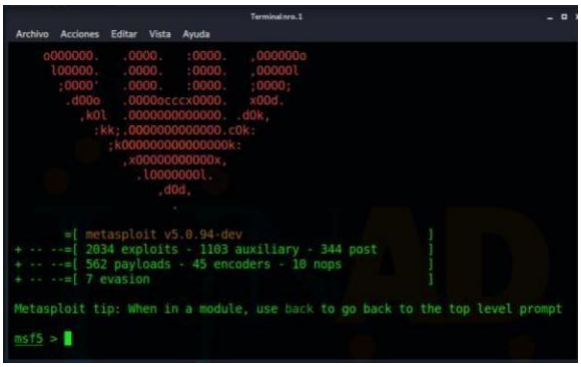


Fuente: Elaboración propia

Este software se valida por medios de la terminal de Kali Linux, teniendo como validaciones la seguridad inicial del sistema operativo como lo es la información de sistema operativo nombre del equipo y conexiones o servicios dentro del equipo que se puede identificar a trasvés de la red y que los usuarios no lo pueden detectar a simple vista ya que hay softwares que se emiten en un segundo plano, y sin autorización de los usuarios administradores.

También utilizamos un exploit de Kali Linux , que es el meta es metasploit-framework es un programa que emplea simulación de ataque s y verificación de permisos a través de varios exploit que infiltran código shell malware que afecta la integridad del sistema operativo teniendo como objetivo la sustracción y creación de parámetros nuevos que pueden ir de crear usuarios hasta de ejecutar programas encriptados para sustraer la información del sistema operativos a través de comandos remotos sin que la víctima tenga conocimiento de esta ejecuciones ya que se instala una conexión clandestina entre la víctima y el atacante.

Figura 23. metaesploit comandos de verificación

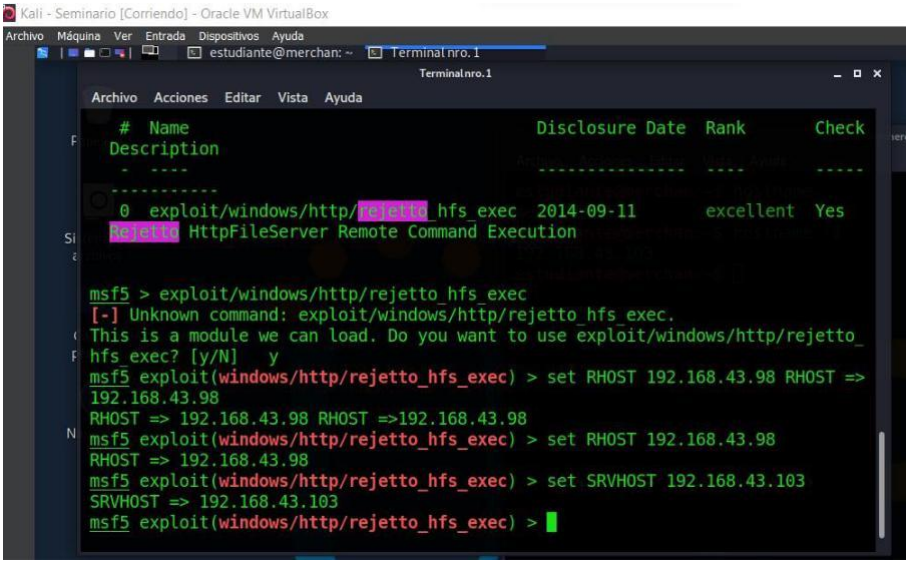


Fuente: Elaboración propia

Análisis del ataque presentado a cada una de las maquinas identificadas.

El ataque que se empleó sobre la maquina es el de metaexploit de insertar a través de un comando de conexión y de envió de script a traves de una conexión apache de un host simulando una página web ataraves de esa conexión. Se envía un comando donde podemos ejecutar varias configuraciones de tipo administrador sin que el usuario sede de cuenta

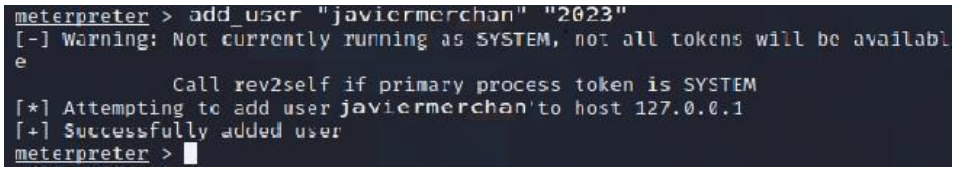
Figura 24. análisis de rejetto



Fuente: Elaboración propia

Luego de ejecutar el scrip internamente al abrir sesión de nuevo en la maquina se pude realizara las verificaciones de conexión través del comando meterpreter, el cual ejecutamos con la configuración desea da en este caso la de crear un usuario local con permisos administrador de ejecución.

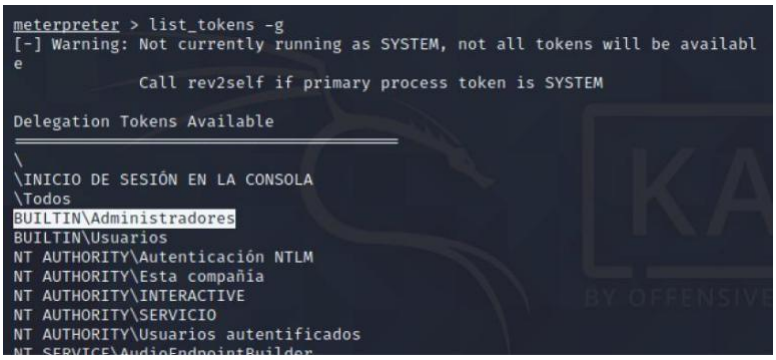
Figura 25. creación de usuario



Fuente: Elaboración propia

Por medio del comando de inserción meterpreter se procede con la asignación del nombre del nuevo usuario y de asignación de permisos

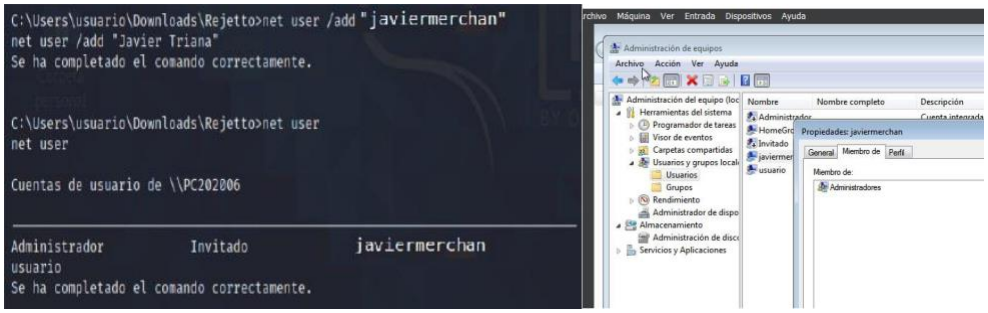
Figura 26. Lista de permisos de usuario



Fuente: Elaboración propia

Se procede con la asignación de permisos de usuario por lo cual se escoge el usuario Javier merchan y se asignan los permisos correspondientes como administrador

Figura 27. Validación de permisos



Fuente: Elaboración propia

Con concluyendo que el comando meterpreter podemos asignar permisos de administrador a cualquier usuario y así instalar programas maliciosos como también ocultar información y controlar el equipo remotamente a través de varios scrips que me ayudaran a asignar protocolos de control de seguridad del equipo.

Figura 26. creacion ataque de scrip shell

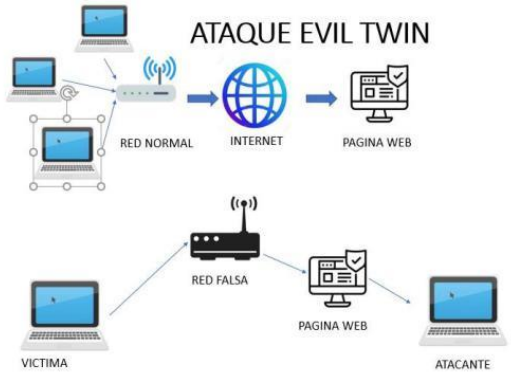
Fuente: Elaboración propia

Como lo evidencia la gráfica anterior cualquier simulación de página web podemos obtener la información de la víctima al desconocer los principios de la seguridad de la información.

Informe de la explotación de vulnerabilidades en el escenario propuesto.

Durante la ejecución del programa de rejetto, teniendo como obettijo habilitar los puertos de conexión del computador haciendo que los usuarios desconocidos manipules el computador, esta vulnerabilidad esta estipulada en a la siguiente referencia CVE-2014-6287.

Figura 27. Gráfico de un ataque rejetto

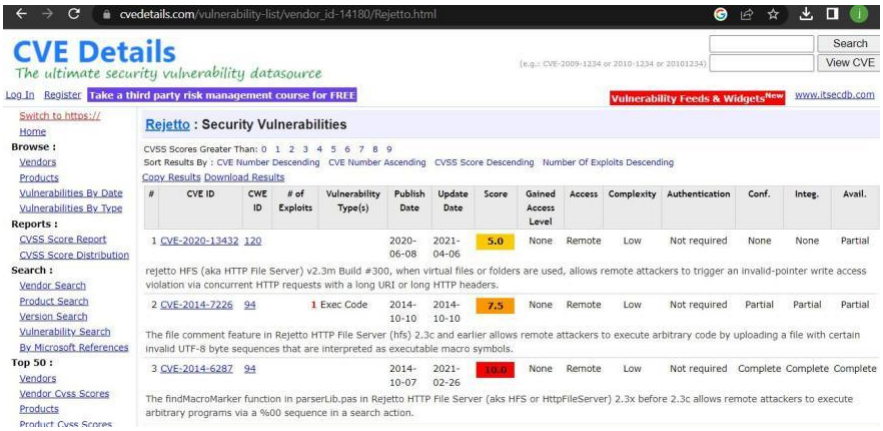


Fuente: Elaboración propia

Referenciado como manipulación de control remota , la acción que el programa tiene en su versión de un puerto epecifico para crear un repositorio virtual,las bases de datos X-Force (95950), Vulnerability Center (SBV-46797) y Exploit-DB (34668), validando que este programa es de nivel alto ya que afecta directamente la programación de los parámetros de seguridad de conexión de redes LAN adicional emple la ejecución de verificación de servicio http y https de manera insegura , tenido como objetivo que el computador este ecpuestoa ataque específicos como lo es los ataques de exploit de la información , adicional la manipulación de sistemas de transferencia de archivos de manera no segura no utilizando certificados de verificación ssl

Figura 3: Vmware instalado con Kali
Fuente: Elaboración propia

Figura 27. validación tipo de vulnerabilidad

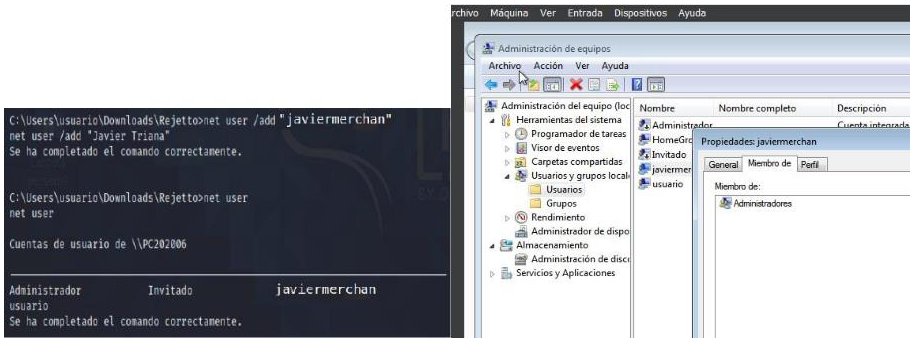


Fuente: Elaboración propia

Evidencia De La Explotación De La Vulnerabilidad Identificada

Por medio de la explotación de la inseguridad comprobamos que al insertar o configurar un nuevo usuario se puede controlar muchas características de Windows 7 en su versión a 64 bit

Figura 28. creación de usuario con privilegios con comandos de Kali linux



Fuente: Elaboración propia

Por lo cual se identifica que el sistema a quedo muy vulnerable o sensible a cambios por tercero teniendo como objetivo la insegura de la información, teniendo en cuenta estas características se evidencia al momento de la creación del usuario sin que el usuario inicial se dé cuenta es decir podemos con la simple creación de este usuario obtener la información almacenada en el equipo y podemos transferirlo por medio de un servicio ftp en el equipo la información más sensible,

Es una taque que se videncia una suplantación de la conexión de la una red falsa de internet teniendo como objetivo que la víctima se conecte a esa red y así poder obtener la información, pertinente al cunetas y a la información del equipo , para poder realizar esta extracción de información el usuario aceptara la conexión a la red no segura por lo cual se establece una entidad de confianza dirigida a las sistemas de información copiando un vínculo en la red , obteniendo una red fraudulenta que impide que los usuarios detecten al configuración y la victima pueda ingresas sus datos en formularios de conexión.

Paso a paso del ataque

para prevenir el ataque se debe de validara la configuración de la seguridad de la red si es una red WAP debería tener el a anexo de skp de protocolo seguridad adicional a las redes más inseguras siempre tiene como característica la terminación web sin contraseña para factibilidad de la conexión.

Análisis Con Acciones Necesarias Para Contener Un Ataque En Tiempo Real

Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

Desarrollo

Análisis con acciones necesarias para contener un ataque en tiempo real

Teniendo en cuenta el análisis anterior del caso y su conclusión se validó en primera medida se validaría el uso de la información enviada o almacenada en el computador, también validaría el uso de la aplicación y la seguridad inicial del sistema operativo en toda compañía debe de tener un antivirus que valida la seguridad local del equipo, adicional también se validaría las cuentas de usuario quienes de esas cuentas que son locales están permitidas, y cuales no están permitida con su respectiva validación de permisos, ya que se valida que el equipo no está dentro de un dominio empresarial y el control de cuentas de usuario es local un grave error en la gestión de usuarios, adicional validaría el tráfico de red ya que los puertos de conexión dentro de análisis de red se videncia una comunicación constante dentro e al empresa dando como respuestas que el usuario tiene instalado un servidor local o similar, validaría adicionalmente para otros equipos si existe otra anomalía similar antivirus y firewall si existe alguna configuración adicional en los equipo softwares instalados en el sistema operativos, también las licencias de sistema operativos y validaciones de licenciamiento de software instalado y validados en la compañía, teniendo en cuenta la restricciones de la red en descargar softwares maliciosos.

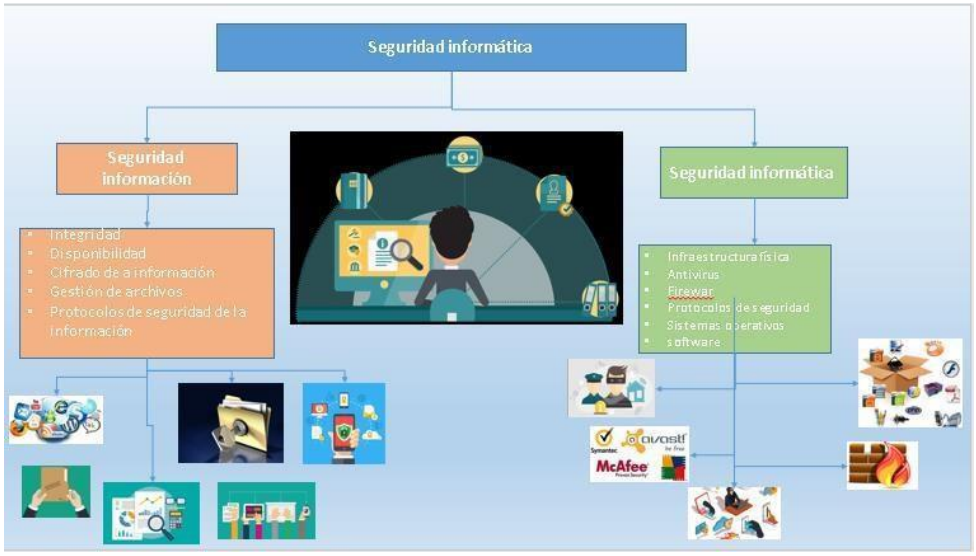
En cuanto a la contención, como primera medida se debe de quitar de la red LAN el equipo, observar su comportamiento en una zona segura y validado por expertos de ciberseguridad, donde se valida la seguridad de la red LAN, adicional la validación de equipo que software estaba interactuando y restringir cualquier software que no está autorizado por la organización, adicional validaría el firewall si existe alguna animalia y procedería con el análisis atravesó de un software en la red de procedencia sospechosa, adicional vigilaría la activación de antivirus y de firewall de todos los equipos se procedería luego a scannear los equipos uno a uno con una herramienta que me valide que los puertos y vulnerabilidades estén cerrados o abiertos, teniendo cada uno con respecto a las políticas internas de la empresa, luego se procedería con validación de restricción de medios tecnológicos extraíbles y de descargar de software a través de la red, también respaldaría todos los servidores y validaría reportes de conectividad y rastreo a través de una herramienta que me permita validar el flujo de información que se atenido últimamente en la red local.

Formas de prevención

- Filtrar la información de temporales
- Validación de estructura de formularios Estructura de código fuente
- Auditorias de versiones de php o de versiones conectores java · Auditoria manuales validando la validación Poc
- Xspear herramienta de análisis de filtros de web donde se detecta los problemas de seguridad páginas web
- Knoxss herramienta donde la principal característica es la validación de información de los formularios de detección donde nos ayuda detectar los códigos Ajax que impide la validación de la información

- BurpSuite es una herramienta que nos ayuda validara el tráfico de consultas así detecta la saturación de código por lo cual es una herramienta de auditoria donde las versiones del hosting son validadas.

Figura 29. seguridad informática



Fuente: Elaboración propia

Propaganda de riesgos

Por medio de un canal de divulgación se da a conocer fuertemente los peligros de no asegurar su información digital, como también la inseguridad en portales de internet en los cuales la comunidad de un país está más propensa a ser afectada por estas situaciones de inseguridad por su desconocimiento en los cuales se refleja una ignorancia en los protocolos de seguridad, con referencia a la información digital

Concienciación sobre los peligros informáticos

Por medio de una capacitación se realizar la retroalimentación de los peligros informáticos teniendo como énfasis la estructura de la información en lo cual se realiza un implementación de casos relevantes en lo cual se abarcara la implementación de un sistema de atención al sistema de información, adquiriendo una concientización de los peligros de informáticos en los cuales se afectar a la información más sensible del banco, también se aplicara campañas informativas al público y a los clientes de los peligros de los delitos informáticos.

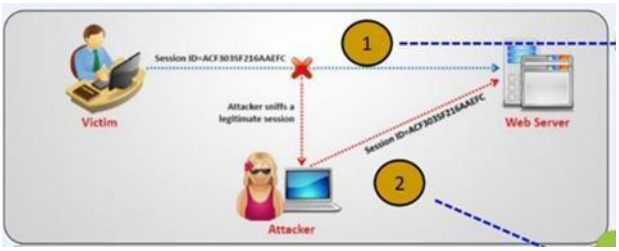
Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática

Teniendo en cuenta el caso anterior se valida que se necesita, una modernización de hardware donde ayudara a controlar las amenazas que provienen de la conexión de la red Lan, con la red global, teniendo en cuenta que estaría direccionando por una persona capacitada en el control de la red perimetral y la red de rea local.

Firewall Serie 9300

Este firewalla tiene una capacidad de más de 160 usuarios tiene varias validaciones de puertos, conexiones certificadas como ejemplo ssl, en entre otros teniendo en cuenta las vulnerabilidades en la red y en la nube ya que cubre el almacenamiento de los archivos de gran velocidad de trasmisión, control de sistemas de información donde los archivos son gestionados adecuadamente a través de una estructura de validación de seguridad informática.

Figura 29. Diagrama de interceptación



Fuente: Elaboración propia

Switch TP-Link TL-SF1048

Este Switch es gestionable para el control de la gestión de la red en el cual se valida la conexión de sistemas de control de puertos de red así también se gestiona la conexión de puertos de red rj45, y se valida la seguridad de puertos abiertos y bloqueo de conexiones ilegales VPN

MM TP-Link Deco Deco M5 V3

Ayudará asegurar las conexiones de wifi seguros ya que posee administración de conectividad y de control de flujos e datos programados en distintas opciones, ya que el control de acceso e dispositivos por wifi asegura ala descarga de archivos malicioso y de conexiones de computadores que no están asegurados en la empresa ya que la gran mayoría tiene un gestor de vulnerabilidades de puertos y de actividades inusuales.

En una gestión empresarial que regula y controla los diferentes parámetros de la seguridad y el manejo informático de un sistema informático, que implementar la regulación de salida y de entrada de información como la verificación y la disponibilidad de los entes reguladores de la información implementado diferentes características que aseguran la integridad de la información como lo es el recurso de la información tecnológica teniendo en cuenta que para los procesos internos de la arquitectura de la información se debe de tener en cuenta los requerimientos de negocio y recursos internos de información

Los cuales se implementa para mejorar la calidad de empresa como también la certificación con los clientes ya que como por ejemplo los bancos tiene empresas que maneja la gestión de la información con contratos exclusivos con empresas certificadas con normas ISO y haya diversos organismos que apoyan la diversidad de la implementación de elementos de infraestructura y de componentes de desarrollo de lenguajes de programación que regulan todo lo referente al control de calidad de la administración de la información

Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

Teniendo en cuenta que para el equipo de blue team se encarga más que todo de las auditorias y de la gestión adecuada de las políticas internas de la compañía con relación a las políticas de la compañía, la diferencia es el equipo blue team tiene procedimientos en el cual ajustan las reglas de seguridad establecidas en el sistema de información y de control de la información, en contraparte el sistema de respuestas de incidentes valida y procede con la incidencias de seguridad informática a través de un sistema de gestión de incidencias que puede ser la mesa de ayuda.

Blue Team

Es un grupo especializado de personas que están capacitadas en la gestión de controles de seguridad dentro de una compañía con los sistemas de protección de la información, donde se especializan en encontrar vulnerabilidades en la gestión de detención de amenazas que se puedan evidenciar en sistemas operativos, se relaciona con las incidencias que se hayan reportado y los reportes de los mecanismos más utilizados como contención de la información.

Los principales objetivos de un equipo son

- Asegurara los sistemas operativos con políticas de restricción
- Implementara mecanismo de flujo de información en un sistema de información
- Gestionará medidas de seguridad en los sistemas internos de la compañía
- Asegurara el buen uso de los pilares de la información · Analizar restos de incidentes
- Validara la ejecución de los controles de seguridad de antivirus · Validara actualizaciones en sistemas de seguridad informática
- Implementación de hardware que ayuden a los sistemas operativos · Generara reportes de niveles de seguridad en los casos más relevantes de los sistemas operativos donde se asegure la información de los sistemas operativos
- Validaciones de gestión de a la información en capacitaciones y auditorias

Equipo de respuesta a incidentes informáticos

Es un grupo que están capacidad para la gestión de incidentes de seguridad esta gestión, que se encarga de solucionar y atender inmediatamente una anomalía en la seguridad de la información , teniendo en cuenta el reporte y la gestión oportuna de los usuarios en cuanto se reporte una incidencia de seguridad tecnológica , dando como objetivo un reporte especializado del control, origen y gestión de la incidencia, a través de una mesa de ayuda que tiene como objetivo la trazabilidad de los incidentes tecnológicas dentro de una organización.

Objetivos

Se hace referencia a las tendencias de nuevas prácticas, y a las políticas de implementación en mejoras de la calidad del sistema de seguridad informática dentro de la compañía como objetivo primordial el sistema de control de incidentes y de implementación de los activos informáticos. validación e implementación de sistemas seguridad de la información

Política de Seguridad de la Información

Esta se refiere a toda medida de restricción y de protección de datos dentro de una empresa u organismos de control de accesos en el cual se verifica la información aportada oportunamente para los datos alojados dentro del sistema informático teniendo como objetivo anulara cualquier incidente inseguro dentro de la política interna de la empresa

Organización de la Seguridad de la Información

Es le organismos donde se evidencia el sistema de control de la información teniendo como objetivo la protección de la información el cual controlara ay adecuara cualquier incidente tecnológico que pueda afectar a la organización y la disponibilidad de la información.

Gestión de activos informáticos

Es toda gestión adecuada al control e inventarios de los activos de la compañía refiriéndose a la información donde se destaca la implementación de medidas de control y de la protección de la información como objetivo principal la estructura de un sistema de atención de información a incidente tecnológicos informáticos

Seguridad de las operaciones y comunicaciones

Se refiere a asegurar la implantación de las telecomunicaciones a nivel de sistemas de información y de infraestructura teniendo como objetivo brindara un soporte oportuno a ala incidencias informáticas presentes sobre la administración de los recursos informáticos y de telecomunicaciones.

Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security"

como propuesta de aseguramiento por parte de un equipo de Blue Team.

Dentro de la gestión del grupo de Blue Team se destaca las actualizaciones de la información de los sistemas más actualizados de control de vulnerabilidades en cuanto a los sistemas más actualizados de ataque que se pueda emplear por lo cual, teniendo el conocimiento previo de los sistemas de información a los cuales se están atacando constantemente optaría por la utilización de CIS ya que la organización tiene mecanismos más actualizados de mitigación de incidencias de seguridad, teniendo en cuenta que haya casos que dentro de la comunidad están bien documentados, lo utilizaría como asesoría en los casos más relevantes teniendo como objetivo la documentación previa de los ataques más actualizados.

Los cuales se implementa para mejorar la calidad de empresa como también la certificación con los clientes ya que como por ejemplo los bancos tiene empresas que maneja la gestión de la información con contratos exclusivos con empresas certificadas con normas establecidas en la comunidad y haya diversos organismos que apoyan la diversidad de la implementación de elementos de infraestructura y de componentes de desarrollo de lenguajes de programación que regulan todo lo referente al control de calidad de la administración de la información.

Por medio capacitaciones a los empleados a un nivel intención sobre la seguridad de la información, adicionando casos reales donde la legislación de Colombia rige con dureza los delitos informáticos donde se destaque la filtración de la información adicional capacitando a los usuarios del sistema sobre el reporte de incidentes de seguridad de información teniendo como ejemplo el sistema de gestión de seguridad de la información.

Educación a cerca de los peligros informáticos que se pueda adquirir a través de los CIS se capacitaría sobre los peligros en los cuales el personal de los bancos y los clientes caen por lo cual los refuerzos de la normatividad de la información, así como el buen manejo de la integridad de los datos es de vital importancia destacando los pilares de la información y así asegurando que el personal tome conciencia de los peligros de la divulgación no autorizada de la información interna de los bancos.

Análisis sobre las funciones y características principales de un SIEM

El SIEM es un conjunto de gestión de incidencias de seguridad informática, teniendo como objetivo la gestión de incidencias dentro de la compañía utilizando, medidas de contención y de validación de la información donde se documentos constantemente los casos a través de un sistema de información donde la capacidad de interacción de los usuarios usuario con el agente del servicio sea de manera mas adecuada en los sistemas informáticos, a continuación se observa las caracterización y flujo de los procedimientos de las incidencias tecnológicas en relación a los sistemas informáticos de la organizaciones.

Figura 31. Gestion De Riesgos Etapas

Fuente: Elaboración propia

Teniendo establecidos la metodología por las diferentes áreas del sistema de control de incidentes se procede con la implementación de la normativa teniendo como objetivo establecer los riegos principales dentro de los sistemas de información de una compañía a entidad donde se establece el siguiente proceso estructurado, adicional es una normatividad certificable por varias entidades en la seguridad de la información.

Identificar los activos informáticos

Son los datos informáticos en el cual se procede con gestión de esta dentro de un sistema de información, por lo cual contiene datos sensibles de la compañía en el cual se establecerá un respaldo de información dentro de la compañía.

Amenazas

Son aquellas deficiencias que tiene un sistema el cual expone a daños de la información, que se puede presentar en el tratamiento de la información teniendo como objetivo obtener la información de forma ilegal.

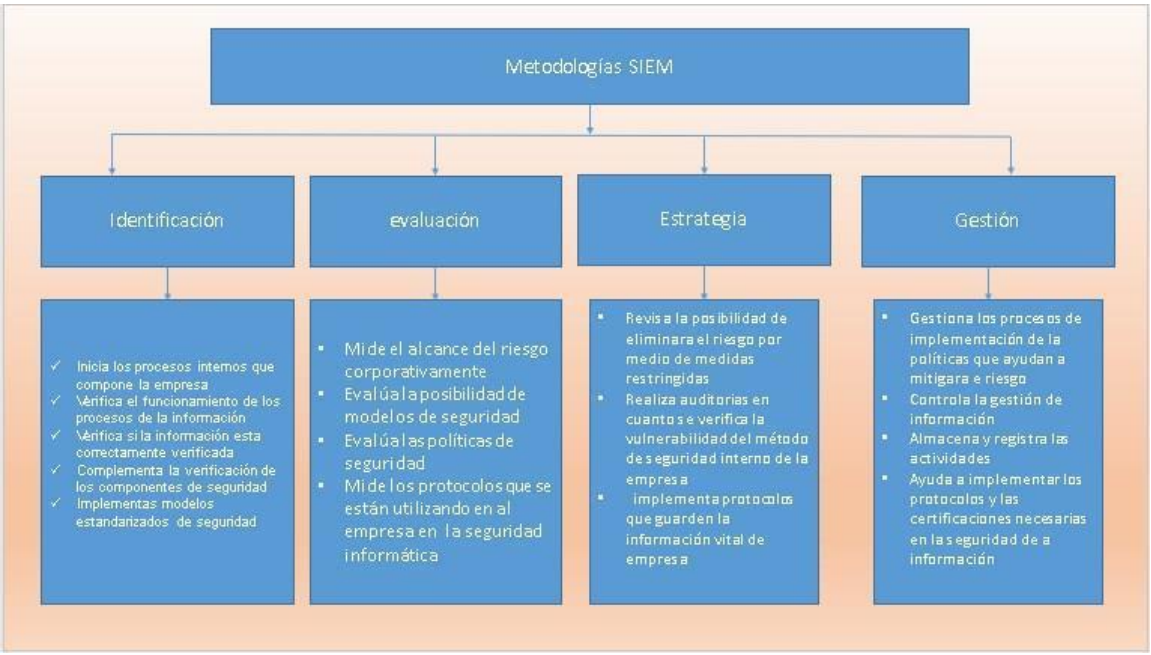
Vulnerabilidades

Es una incidencia que se presenta ay que puede afectar la información del sistema de información dentro de la compañía teniendo como objetivo afectara el proceso interno de la compañía en cuanto a el tratamiento de la información sensible de los activos informáticos.

Requisitos legales

Son la normas internas y externas que rigen la compañía en cuanto a los procesos de los activos como disponibilidad de la información atendiendo al proceso interno de la compañía. Asegurando la información vital de los usuarios y de la infraestructura tecnológica que posee la compañía o las entidades privadas o públicas.

Figura 32. Metodologia SIEM



Fuente: Elaboración propia

Informe de elección de 3 herramientas que permitan contener

ataques informáticos

Los mecanismos de control de vulnerabilidades se identifican que en la actualidad hay varias herramientas de sistemas y software en los cuales ayudan a la mitigación de una vulnerabilidad en los cuales evidenciamos que su documentación está referenciados a los sistemas informáticos.

Que se implementa en un sistema informático el cual estaría estructurado en capas de comunicación tecnológicas los cuales envían y reciben información es importante detectar estas anomalías e identificara para mitigar sus acciones dentro de un sistema informático ya que generando una repuesta inmediata se generar una cultura de auto protección y de gestión del riego informático donde se destaca la cateterización de protocolos de seguridad así como políticas internas y externas para su posterior aplicaciones a la información más relevante de una entidad como se observa en los ciberataques más comunes que se observa.

Herramientas de contención

A continuación, nombraremos 3 herramientas de mitigación y control de vulnerabilidad que ayudaran en caso de presentarse una anomalía de seguridad de la información en tiempo real.

Malwarebytes

Es un programa que ayuda a eliminar cualquier virus y inspecciona también anomalías de seguridad informática como lo es los puertos abiertos adicional protege los archivos que hace una búsqueda exhaustiva de virus que se pueda presentar en los ordenadores y los repositorios que están ubicados en la red adicional tiene una hermanita de validación de trafico de red en el cual se valida la implementación de scanner en documentación n al nube y validación de sistemas de información, al actualizarse constantemente por su sistema operativo y valida también los documentos antiguos con relación a otro computadores.

Endpoint disk encryption

Es una gente que ayudara a encriptar todos los documentos en relación a los equipos y su flujo de información interna ya que al transferir a la red encripta y valida la información dependiendo de un etiquetado de medida de trasferencia en público, confidencial, privado, por lo cual nos ayuda a que cualquier documento extraía de una forma ilegal no le sea fácil de validar su contenido inicial si no es a través de una herramienta de encriptación que le ayudara a visualizar la información contenida en los archivos de trasferencia como la siguiente referencia de definición y uso de endpoint [12]"The underlying components of all endpoint encryption solutions are fairly similar. The encryption algorithms in common use today – such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) – are public protocols that anyone can use. These encryption algorithms are believed to be secure against attacks by modern computers.".

Servidores NAS

Es un servidor especifico de backup de archivos donde un equipo está infectado con un malware esta aplicación hace una copia actualizada y sincronizada de los documentos para luego ser actualizados nuevamente en el equipo para dar continuidad de los archivos que no están infectados.

12 (S/f-b). Checkpoint.com. Recuperado el 14 de noviembre de 2023, de https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-security/what-is-endpoint-encryption/#:~:text=Endpoint%20encryption%20uses%20encryption%20algorithms,sensitive%20data%20against%20p%20hysical%20threats..

En la actualidad existen tendencias tecnológicas que cada vez está más sujeta a la inseguridad ya que para algunas personas la seguridad de la información es muy valiosa, ya que para la implementación de protocolos de seguridad se está implementando en políticas que cada vez expande el conocimiento previo de las personas teniendo en cuenta que los sistemas de información manipulan la información de los usuarios

Por lo cual el análisis ayudara a identificar los siguientes parámetros tecnológicos

- Ataques externos
- Ataques internos
- Normas de seguridad informática
- Regulación de datos
- Manejo adecuado de la información aplicada a los sistemas informáticos
- Disponibilidad de la información
- Integridad de los datos
- Confidencialidad de la información

Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam

Teniendo en cuenta el desarrollo de la técnicas y procedimientos del sistema de red team y blue team, se estipulan varios aspectos que ayudarían al fortalecimiento de la recolección principal de la información, en los procesos de la exploración.

Red team

Estaría referenciado en ataques de versiones nuevas de phishing y control de dispositivos de medios magnéticos así como variaciones de diversos dispositivos de almacenamiento , adicional m la validación de sistemas red teams en la nube ya que en los últimos años se ha evidenciado una aumento significativo de la aplicaciones iCloud por tal motivo es vital el refuerzo de seguridad en estos servicios como referencia en el siguiente top 10 de vulnerabilidades [13]"*A cloud cryptomining attack is a type of cyber attack in which attackers use cloud computing resources to perform cryptomining without the knowledge or consent of the cloud provider or the owner of the resources. Cryptomining is the process of using computing resources to solve complex mathematical problems in order to verify and validate transactions on a blockchain network."*

Simulación de ataques de phishing a correos externos e internos

Esta simulación ayudaría implementara mecanismos de control en los sistemas de dominios que son suplantados por el ataque phishing, como el envío y recepción de correos que no están dentro del dominio y se están utilizando como reglas de almacenamiento.

Simulación de ataque de Evil Twin

Esta simulación ayudaría a identificar los equipos que simularían a través de red de internet una subred y así clonara las páginas de la compañía para la validación de credenciales de usuario, como nos indicaría la implementación de reglas de control de accesos dentro de red de internet teniendo como base la exploración de varios mecanismos de seguridad informática [14]"*Dans ce scénario, la red team est l'équipe dite externe chargée de réaliser un test d'intrusion. Celle-ci doit se comporter de la façon la plus réaliste possible c'est-à-dire un attaquant déterminé ciblant une entreprise. Contrairement à un pentest classique avec un scope spécifique, la plupart des moyens sont bon pour s'introduire dans une organisation. Ces derniers seront amenés à faire du social engineering, pénétrer physiquement dans les locaux sans éveiller les soupçons, réaliser leurs propres exploits/payloads/malwares… leur périmètre d'attaque est vaste. Pour que l'attaque soit réalisée dans des conditions optimales, ces derniers n'auront aucune information sur les systèmes de l'entreprise (du moins fournie officiellement par le client)."*

---

[13] Top 10 cloud attacks and what you can do about them. (2023, enero 4). Aqua; Aqua Security. https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/

[14] Red team VS blue team. (s/f). Lutessa.com. Recuperado el 14 de noviembre de 2023, de https://www.lutessa.com/?p=5524

Es importe reconocer que actualmente se está necesitando más almacenamiento en la red para almacenamiento de tipo backup de la información vital de la empresa es por eso que cada vez se requiere más conocimientos de los servicios cloud en Colombia tenemos como principal dificultad que la localización de los repositorios de la red no están referenciándose y es común que los usuarios olviden el ingreso de los repositorios o tengan dificultades a la hora de ingresar a la plataforma es de vital importancia determinara los protocolos de almacenamiento y restringir en lo posible la duplicidad de documentación antigua teniendo como resultados versiones que ocupan un espacio y afectar drásticamente la capacidad de la red, es como se referencia en este artículo [15]"*Esta información requiere un tratamiento específico durante todo su ciclo de vida, ya que se deben preservar sus propiedades de autenticidad, fiabilidad y usabilidad y en algunos casos confidencialidad . Pueden ser ficheros de documentos, hojas de cálculo o PDF, bases de datos, formularios web, archivos de imágenes, video o multimedia, archivos CAD, XML, SMS, páginas web, archivos de log, etc*

Teniendo como base lo anterior es necesario investigar más a profundidad los casos más relevantes donde se tenga en cuenta los servicios cloud que ofrecen los operadores en Colombia, resaltando las dificultades que se evidencia en la ciberseguridad del servicio.

Blue team

Las empresas establecen que cada día haya cada vez más seguridad de la manipulación y divulgación de la información por lo cual las empresas se están capacitando y certificando para la seguridad informática por lo cual están teniendo tendencias de seguridad guardando los pilares de información, que es integridad, disponibilidad, confidencialidad ya que en estos pilares se realiza la gestión ordenada y adecuada de la manipulación de datos de una persona o empresa en las organizaciones tiene como obligación capacitar y tener un departamento que vigile cualquier irregularidad que pase con los datos de los clientes como los datos de las personas que tenga un fin especifico tales el caso de que bloqueos y contratos como cláusulas de confidencialidad están sujetos a disposiciones de la empresa con validación de los usuarios, características que tienen como objetivo la protección de un sistema de información es así que se tienen un campo dentro de la informática especializada en implementar políticas que protegen la integridad de la información dentro de un sistema informático , teniendo en cuenta que cada día hay nuevas tendencias tecnológicas que no afianza con la seguridad ya que es de vital importancia la integridad de un sistema informático.

[15] Amenazas y riesgos de la nube. (2020, febrero 20). Evaluandosoftware.com. https://www.evaluandosoftware.com/ciberseguridad/amenazas-riesgos-la-nub

Actualización y modernización

La actualización de estos protocolos se referencia la modernización de los ordenadores personales y empresariales para ayudar a la vida del usuario con la interacción de la información por tal motivo se están modernizando constantemente estos protocolos con referencia al protocolo estándar de trasmisión de red, cubriendo las nuevas necesidades con referencia al uso explícito de la información en la red.

Estructura organizacional de la información

Los lineamientos especificado en la organización dentro de la ISO 27001 que regula a calidad de la seguridad de la información dentro de una entidad o empresa lo cual gestión y controla en su mayoría la calidad de la seguridad de los archivos y de los datos utilizados dentro de la empresa, con esta normatividad se da como garantía de que la empresa o organización tiene como principal objetivo la integridad de la información, Estrada establecidos dentro de los servicios cloud estandarizados en el sistema pvha.

La normatividad 27001 nos da un enfoque estructural de las normativas y políticas que se establece en el sistema de gestión de la información teniendo como base principal, los pilares de la información que son la integridad, la confidencialidad, la disponibilidad en la ISO 27001 establece los parámetros estructurales de la gestión de la seguridad informática teniendo en cuenta, Por medio del sistema de calidad PHVA que es la estructura más vital teniendo como ejemplo la incidencias de los casos más relevantes de la seguridad informática en la compañía.

En el planificar, identificar, implementar y en verificar los procesos de los activos informáticos de la empresa o entidad pública teniendo como objetivo mitigar los incidentes de las seguridad informática que pueden tener riesgos significativos dentro de la compañía, adquiriendo un sistema de control de incidencia más eficaz, teniendo el control de los sistemas de información el cual se evidencia un control total de los datos de la compañía, se puede implementar este protocolo a cualquier compañía ya que su estructura es ajustable a cualquier compañía que tenga un majeo de información importante.

Recomendaciones para el planteamiento de estrategias que

permitan endurecer los aspectos de seguridad en una organización

La implementación de la normativa ISO27001

Teniendo establecidos la metodología por las diferentes áreas del sistema de control de incidentes se procede con la implementación de la normativa teniendo como objetivo establecer los riegos principales dentro de los sistemas de información de una compañía a entidad donde se establece el siguiente proceso estructurado, adicional es una normatividad certificable por varias entidades en la seguridad de la información.

Identificar los activos informáticos

Son los datos informáticos en el cual se procede con gestión de esta dentro de un sistema de información, por lo cual contiene datos sensibles de la compañía en el cual se establecerá un respaldo de información dentro de la compañía.

Amenazas

Son aquellas deficiencias que tiene un sistema el cual expone a daños de la información, que se puede presentar en el tratamiento de la información teniendo como objetivo obtener la información de forma ilegal.

Vulnerabilidades

Es una incidencia que se presenta ay que puede afectar la información del sistema de información dentro de la compañía teniendo como objetivo afectara el proceso interno de la compañía en cuanto al tratamiento de la información sensible de los activos informáticos.

Requisitos legales

Son la normas internas y externas que rigen la compañía en cuanto a los procesos de los activos como disponibilidad de la información atendiendo al proceso interno de la compañía. Asegurando la información vital de los usuarios y de la infraestructura tecnológica que posee la compañía o las entidades privadas o pública

los riegos informáticos

los riegos que los sistemas de almacenamiento, tiene como referente, el manejo de la plataforma y su infraestructura y también al desconocimiento de la plataforma que los usuarios tienen de la plataforma y sus servicios.

Los servicios que establecen la protección de la información teniendo en cuenta las anomalías y las vulnerabilidades más comunes que en el cual se establece las siguientes vulnerabilidades.

Vulnerabilidades más comunes

- Pérdida o fuga de información
- Secuestro de sesión o servicio
- Riesgos por desconocimiento
- Accesos de usuarios con privilegios
- Incumplimiento normativo
- Pérdida o fuga de información

Esta vulnerabilidad está presente en los casos donde los usuarios por desconocimiento y por el manejo inadecuado de la plataforma, por lo cual se evidencia una perdida significativa en de la información en los procesos, por lo cual los prestadores del servicio tienen la obligación de capacitar a los usuarios en el funcionamiento de la plataforma, como también especificar el riesgo de la información en ala arquitectura de la nube en el funcionamiento de transferencia de los archivos en tiempo real.

Ejemplos:

- Deficiencia en las claves de acceso
- Derivación de roles de usuarios no contemplados

Medidas de contingencia

- Campañas de divulgación de la plataforma
- Campaña de cambio constante de claves
- Realizar aseguramiento de la información

Accesos de usuarios con privilegios

Este es un ataque en el cual se infiltra las credenciales de usuarios de administración a la plataforma siguiendo el sistema de información en la plataforma teniendo como objetivo la implementación del cambio de acceso de la información por lo cual se establece que las credenciales se implementan en el sistema de información.

Ejemplos:

- Error ingreso no autorizado
- Filtración claves de acceso de la plataforma
- Error de eliminación de usuarios admin

Medidas de contingencia

- Prevención de claves de administración
- Directivas de confirmación de usuarios
- validación de cambios de administración en la plataforma

Incumplimiento normativo

Esta es una incidencia del soporte de la plataforma teniendo como objetivo el mal manejo de la información en la plataforma como también el acceso, adicional esta incidencia hace referencia a la infraestructura de plataforma más como el almacenamiento, este incumplimiento hace referencia a los usuarios y a las políticas de contingencia de la plataforma con los proveedores estipulados en los contratos de servicios de adquirir el servicios y soporte de este.

Ejemplos:

- Error ingreso no autorizado
- Filtración claves de acceso de la plataforma
- Error de eliminación de usuarios Administradores

Medidas de contingencia

- Prevención de claves de administración
- directivas de confirmación de usuarios
- validación de cambios de administración en la plataforma

según la referencia de aspectos tecnológicos en seguridad informática CIS, nos recomienda obtener varias referencia bibliografías de casos de implementación de seguridad informática en las políticas internas de verificación en auditorias de aspecto de control de la información según su prioridad en los diferentes procesos que pasa la información [16]“PoliciesThe Kubernetes CIS benchmark recommends specific policies for Kubernetes elements like RBAC, pods and the container network interface (CNI), to improve security.RBAC, Service Accounts and Admission ControlThe following table summarizes recommendations for the RBAC and Service Accounts.Policy Pertains To Recommended Policy cluster-admin role Only use where required secrets Ensure minimal access”

[16] Kubernetes CIS Benchmark: Best practices in brief. (2021, febrero 8). Aqua; Aqua Security. https://www.aquasec.com/cloud-native-academy/kubernetes-in-production/kubernetes-cis-benchmark-best-practices-in-brief/

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad

Evidenciando el resultado del estudio de la seguridad informática en los sistemas de información de Colombia ,se estableció que en la actualidad la normatividad de los procesos internos de la información son ejecutados para el aseguramiento de la información teniendo en especial protección la integridad y la disponibilidad de la información en los sistemas de seguridad informática en Colombia teniendo como objetivo la validación de las políticas que cada proveedor implementa para asegurar y resguardar la información de compañías y de instituciones que requieran estos servicios.

El presente trabajo identifico las vulnerabilidades y riegos informáticos a los cuales los sistemas informáticos son expuestos, al implementar un sistema de consulta de la información en la nube, identificando sus posibles medidas de mitigación que están establecidas en los procesos internos de una compañía en la actualidad como política de tratamiento y protección de la información ,en donde la información es almacenada en la infraestructura que ofrecen los diferente proveedores de servicios computing cloud en Colombia.

Se debe de restructurara la validaciones en sistemas de app ya que hay restricciones pero no controlan el flujo de información en los dispositivos móviles es la estructura que nos referenciados en la implementación de transferencia de la información según [17]"A security policy (also called an information security policy or IT security policy) is a document that spells out the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data. Security policies exist at many different levels, from high-level constructs that describe an enterprise's general security goals and principles to documents addressing specific issues, such as remote access or Wi-Fi use."

[17] Grimmick, R. (2022, junio 29). What is a Security Policy? Definition, Elements, and Examples. Varonis.com. https://www.varonis.com/blog/what-is-a-security-policy

Recomendaciones

Actualizar las medidas de contención a las vulneraciones que presentan los sistemas de información de la compañía teniendo especial atención en el respaldo de la información, así como el tratamiento de la información almacenada

Adquirir una cultura de sensibilidad de la información y caracterización de los riesgos informáticos que afectan la información a los equipos de cómputo.

Aplicar las políticas y controles en los usuarios quienes establecen la responsabilidad de la información de los protocolos de seguridad dentro de la compañía en Colombia aplicando la normatividad de la ISO 27001 sobre los servicios de terceros que afectan o respaldan la información de la compañía.

Documentar los casos más relevantes que obstruya la práctica de los peligrosas de la información, que están relacionados en los sistemas de información en las compañías en Colombia verificando la gestión de riesgos y sus controles de mitigación.

Afianzar términos y protocolos que en Colombia se han venido implementado al desarrollo constructivo de la tecnología en Colombia, apoyado por el ministerio de tecnología con soporte en las leyes que estipulan el manejo de la información digital de los sistemas informáticos, así como la responsabilidad de los usuarios y proveedores que gestionen la información de una compañía o institución gubernamental

Conclusiones

Este trabajo observamos que el propósito general era dará solución a las interrogantes propuestas a través de la lectura inicial acerca del curso de equipos estratégicos en ciberseguridad: red team & blue team lo cual nos da una perspectiva de como el desarrollo del análisis y la gestión del riegos en la seguridad informática que ayuden a la implementación de estrategias de gestión de riesgos, con referente a los últimos años, nos permitió afianzar los procesos de integración de las diferentes utilidades de las cuales se hace referencia la políticas de diferentes normativas utilizadas para la gestión de la información.

Se estructura un sistema de registro de riesgos en el manejo de la información donde se hace evidencia la mitigación y protección de la información en los sistemas de información, como también un esquema detallado de la políticas y normativas que ayudan a mitigara y respaldara la información de los usuarios de los sistemas de información, apoyándose en la normativa del sistema de gestión de la seguridad de la información, realizando una estudio minucioso de la seguridad informática con estudio de equipos de vulnerabilidad red team.

Se realizo la divulgación de la normatividad de sugeridos para la contención según los equipos blue team, tenido especial atención a las políticas que cada compañía ofrece , cuando se opta por la validación de la seguridad informática, apoyados por la normativa vigente de la política de la información que esta referenciada en la constitución política de Colombia, estableciendo un conocimiento más detallado de la normatividad de estos servicios que en Colombia están vigilados por la superintendencia de industria y comercio.

De acuerdo con los resultados obtenidos en el análisis de la seguridad informática del manejo de la información en los diferentes procesos de una compañía, se estableció la documentación que ayudara a los usuarios para identificar los riegos a los cuales se exponen en una la red teniendo en cuenta las vulnerabilidades más relevantes en la actualidad.

Enlace al video de sustentación

https://youtu.be/0IGgJez7YCk

BIBLIOGRAFÍA

Amenazas y riesgos de la nube. (2020, febrero 20). Evaluandosoftware.com. https://www.evaluandosoftware.com/ciberseguridad/amenazas-riesgos-la-nube/

Código Civil Artículo 1519. Objeto ilicito. (s/f). Leyes.co. Recuperado el 14 de noviembre de 2023, de https://leyes.co/codigo_civil/1519.htm

Constitución Política De Colombia. (s/f). Justia.com. Recuperado el 14 de noviembre de 2023, de https://colombia.justia.com/nacionales/constitucion-politica-de-colombia/titulo-vii/capitulo-1/

Cuervo, J. (2009, julio 29). Ley 1341 Principios y conceptos sobre la sociedad de la información - Informática Jurídica. Informática Jurídica. https://www.informatica-juridica.com/ley/ley-1341-principios-conceptos-la-sociedad-la-informacion/

Grimmick, R. (2022, junio 29). What is a Security Policy? Definition, Elements, and Examples. Varonis.com. https://www.varonis.com/blog/what-is-a-security-policy

Kubernetes CIS Benchmark: Best practices in brief. (2021, febrero 8). Aqua; Aqua Security. https://www.aquasec.com/cloud-native-academy/kubernetes-in-production/kubernetes-cis-benchmark-best-practices-in-brief/

Ley 962 de 2005 - Gestor Normativo. (s/f). Gov.co. Recuperado el 14 de noviembre de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=17004

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_0599_2000_PR007]. (s/f). Senado de la Rep&#65533;blica de Colombia. Recuperado el 14 de noviembre de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr007.html

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s/f). Senado de la Rep&#65533;blica de Colombia. Recuperado el 14 de noviembre de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Normatividad sobre delitos informáticos. (2017, julio 25). Policía Nacional de Colombia. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Política de Protección de Datos Personales. (2021, agosto 4). Ministerio de Ambiente y Desarrollo Sostenible. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

Red team VS blue team. (s/f). Lutessa.com. Recuperado el 14 de noviembre de 2023, de https://www.lutessa.com/?p=5524

Rejetto : Security vulnerabilities, CVEs. (s/f). Cvedetails.com. Recuperado el 14 de noviembre de 2023, de https://www.cvedetails.com/vulnerability-list/vendor_id-14180/Rejetto.html

Top 10 cloud attacks and what you can do about them. (2023, enero 4). Aqua; Aqua Security. https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/

(S/f-a). Gov.co. Recuperado el 14 de noviembre de 2023, de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

(S/f-b). Checkpoint.com. Recuperado el 14 de noviembre de 2023, de https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-security/what-is-endpoint-encryption/#:~:text=Endpoint%20encryption%20uses%20encryption%20algorithms,sensitive%20data%20against%20p%20hysical%20threats..