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

JORGE ANDRES DORADO CAMPO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
PIENDAMO CAUCA
2020

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

TUTOR
JHON FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
SEMINARIO ESPECIALIZADO
PIENDAMO CAUCA
2020

RESUMEN

En el siguiente documento se busca realizar un análisis a la normatividad colombiana y el estado actual de la legislación en entorno a los avances de seguridad informática realizando recomendaciones que buscan endurecer y dar mayor castigo a los delitos informático cometidos.

Dentro del red team y blue team es necesario conocer como los pro y los contra de la ley para ello en Colombia se diseñó la ley 1273 DE 2009 la cual nos permite conocer los delitos que son castigados con aislamiento en centro penitenciario o pago bajo fianza, dentro de esta ley se encuentran enmarcadas las diferentes tipologías de delitos que existen o que son tipificados mediante los artículos.

El bluen team también conocida como la última línea de defensa esto para mantener vigilante en busca de actividad sospechosa, es el encargado de la identificación e implantación de medidas para responder a un ataque relacionados con incidentes de seguridad mediante recomendaciones que puede tomadas en cuenta para al momento de que ocurran o en método de prevención.

TABLA DE CONTENIDO

GLOSARIO

Amenaza: circunstancia que tiene como potencial hacer daño o causar perdida de información destrucción o divulgación

Antispam: aplicación informática que se encarga de eliminar correos no deseados Malware, código abierto y malicioso cuya acción es dañar un sistema o u mal funcionamiento

Ransomware: programa que bloquea el equipo y pide dinero a cambio de regreso de información.

Phishing: técnica utilizada para obtener información confidencial, haciéndose pasar por información legitima.

Antivirus: programa utilizado para eliminar software malicioso.

Cracker: persona con conocimientos elevados en sistemas informáticos para romper la seguridad de los mismos.

Cifrado: proceso de codificación de información importante.

Encriptación: es el proceso para volver ilegible información mediante el uso de clave

Exploit: error de software que presenta un fallo de seguridad.

Freeware: salida no controlada de información, es todo aquel software legal distribuido de forma gratis.

Gateway: es un ordenador que permite la comunicación entre distintos tipos de plataformas

1 INTRODUCCION

Para dar la bienvenida al lector, se indica como punto inicial de este documenta el marco legal que comprende los delitos informáticos, actualmente la seguridad informática es esencial en cualquier entidad, sin embargo el avance que se ha visto es lento en consideración con la gran evolución de la tecnología, el riesgo y las amenazas están listas para atacar las vulnerabilidades en cualquier sistema de información, es importante hacer uso de herramientas y controles que permitan mitigar los riesgos a los que se expone la información en el uso de aplicaciones web.

La seguridad en los datos al momento de intercambiarlos de un cliente hacia un servidor o entre dos máquinas se ha convertido en un tema complejo debido a la incontable pérdida de información a causa de los delincuentes en la red.

El trabajo presentado plantea un enfoque para la detección de vulnerabilidades con base a la identificación de vulnerabilidades de servicios activos.

2 DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Las nuevas tecnologías brinda diferentes formas de engaño, suplantación y robo de identidad, según la marca kaspersky registra 45 ataques por segundo en américa latina este tipo de ataques se da explotando una vulnerabilidad ya afectada, Colombia como el 3 país con más afectaciones por malware móvil[1].

Según información recopilada se espera que para el 2020 el número de contraseñas aumenté hasta alcanzar los 300 billones, el 43 % de los ataques afecta a los negocios pequeños, según el FBI ocurre 4.000 ataques ransomware por día se estima que hay un ataque de este tipo cada 14 segundo[2]

En la actualidad el sistema operativo más atacado es Windows actual mente se revelo fallas de vulnerabilidad tanto en sus versiones recientes como lo es win 10 y server 2016-2019, por problemas de salud pública muchas personas optaron por trabajar de forma remota con lo que se ve afectado la seguridad y el aumento de ataques por fuerza bruta al protocolo de escritorio remoto

[1] SD, A. (2019). *Kaspersky registra 45 ataques por segundo en América Latina.* Obtenido de https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

[2] (NICOLAS POGGI. (2018). *24 Estadísticas de Seguridad Informática que Importan en el 2019.* informe. Obtenido de https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

3 MARCO CONCEPTUAL

VULNERABILIDAD. Una vulnerabilidad informática es una debilidad del software o hardware que permite realizar ataques, una amenaza puede ser interna como externa una amenaza es la probabilidad de vulneración convirtiéndola en daños esto identifica como riesgo, también existe otro tipo vulnerabilidad de dia cero, vulnerabilidad de diseño y vulnerabilidad por el factor humano

RIESGO. Se comprende en la identificación de activos informáticos sus vulnerabilidades y amenazas que se encuentran expuestos y asi aceptar disminuir evitar la ocurrencia del riesgo

AUTOMATIZACIÓN. Un conjunto de tareas informática, métodos que sirve para realizar tareas repetitivas en un computador algunos de los métodos para la automatización es la programación

ANALISIS DE VULNERABILIDADES. Es un servicio por el cual se revisa a través de herramientas software las debilidades y fortalezas ante un conjunto de amenazas ya conocidas

3.1 MARCO LEGAL

LEY 1273 DE 2009. Por la cual se modifica el código penal y se crea un nuevo bien jurídico llamada protección de la información y datos, y se preservan integral los sistemas que utilizan tecnologías de información, el 5 de enero de 2009 el congreso de la republica dio a conocer la lay 1273 y se crea un nuevo bien tutelado llamado protección de la información y delitos informáticos por lo cual es importante que las empresas se protejan para evitar que ocurran

ARTICULO 269A ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que por ingresar sin autorización a un sistema informático en parte o en todo, o con medida de seguridad incurrirá en una pena de prisión de 48 a 96 meses

ARTICULO 269B OBSTACULIZACIÓN ILEGITIMA DE UN SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIONES. El que son estar autorizado impida u obstaculicé un sistema informático o en una red

ARTICULO 269C, INTERCEOTACION DE DATOS INFORMÁTICOS. Sin orden judicial previa intercepte datos informáticos de su destino u origen de emisiones de un sistema informático incurre en una pena de 36 a 73 meses de prisión

ARTICULO 269D, DAÑO INFORMÁTICO. El que sin permiso destruya dañe o altere datos informáticos en un sistema de almacenamiento de información, sus partes o componentes lógicos incurre en una pena de prisión de 48 a 96 meses

ARTICULO 269E, USO DE SOFTWARE MALISIOSO. El que sin permiso, produzca trafique adquiera distribuya vende en todo el territorio nacional incurre en una pena de 48 a 96 meses

ARTICULO 269F, VIOLACIÓN DE DATOS PERSONALES. El que sin permiso para hacerlo o estar facultado obtenga información obtenga extraiga información para bien propio o de un tercero incurre en una pena de 48 a 96 meses de prisión[3]

[3] T., José Camilo Daccach. delta acesores. [En línea] https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D..

4 OBJETIVO GENERAL

Realizar un análisis a las herramientas técnicas y la ley 1273 de 2009, utilizadas en el red team y blue team a partir del seminario de profundización

4.1 OBJETIVOS ESPECIFICOS

- Realizar un análisis sobre la importancia de la normatividad colombiana en delitos informáticos
- Identificar las principales fallas que puede tener una organización en cuestión de seguridad informática
- Realizar recomendaciones al momento de tener un ataque de seguridad informática

5 DESARROLLO DE OBJETIVOS

DESARROLLO DE OBJETIVO 1

5.1 REALIZAR UN ANÁLISIS SOBRE LA IMPORTANCIA DE LA NORMATIVIDAD COLOMBIANA EN DELITOS INFORMÁTICOS

La 1273 de 2009 en Colombia es relativamente nueva para la cantidad de delitos que se dejan pasar dado al poco conocimiento de las personas al momento de declarar así como existen los delitos informáticos también existen los medios para realizar las denuncias informáticas es por eso que la policía nacional colombiana estableció la página web, https://caivirtual.policia.gov.co/ en donde encontrara los encales necesarios para realizar las denuncias sobre los delitos a los que haya siso victima

En Colombia se considera un delito informático a la apropiación indebida de información confidencial almacenada en un computador, usb, correo electrónico o dispositivo móvil

Ley 1273 de 2009. Por la cual se modifica el código penal y se crea un bien jurídico tutelado llamado, de la protección de la información y los datos

- Artículo 269ª. Al que ingrese o se mantenga dentro de un sistema de información vigilado o con un nivel de seguridad del propietario legitimo

- Articulo 269B. el que de manera ilegal ingrese o interrumpa su funcionamiento o la recopilación de información y su acceso normal

- Articulo 269C. De manera ilegal intercepte o capture información sin una previa autorización o de un tipo de red que sea utilizada para el trasporte.

- Articulo 269D. Destrucción o daño de información o sistema informático o de sus componentes lógicos.

- Articulo 269E. El uso venta distribución de software malicioso o programas con efectos dañinos.

- Articulo 269F. El trafico la venta la extracción o divulgación de información personal contenido en bases de datos o medios magnéticos.

- Articulo 269G. la suplantación de páginas web captura de datos, modifique sistemas de captura de información, nombres de dominio de forma que pueda confundir a los usuarios que lo utilicen.

- Articulo 269I. El hurto de la información por medios informáticos.

- Articulo 269J la transferencia no consentida de dinero o activos perjudique a alguien será sancionado con la pena más alta.

En Colombia fue de gran avance que se tomara en cuenta la informática como medio para la ejecución de delitos ha sido un poco lento el desarrollo de esta ya que tiene más de 10 años de vigencia y no ha sido actualizadas mientras que los delincuentes informáticos se actualizan constante mente, teniendo en cuenta el que en su tiempo de actividad la ley no ha sufrido cambio alguno, los vacíos legales que dela la ley 1273 permite que los delincuentes puedan evadir las sanciones ya sea penales o económicas y se amparen en la falta de instrumentalización o en la ambigüedad

En el año 2007 se presentó el primer proyecto de ley relacionada con delitos informáticos cuyo beneficio sea la protección de la información y la creación de un nuevo bien jurídico para la protección de la información

En la actualidad en Colombia se cometen más delitos informáticos de los que se tiene conocimiento los años de más incremento se dieron entre el 2012 y 2015 el sexting y ciberbullying smishing

Análisis de los delitos informáticos frente a la ley 1273

El crecimiento de los delitos informáticos aprovechando el uso de las TIC,S teniendo él cuenta el fácil acceso a las tecnologías y a las redes wifi gratuitas más fácil será que los datos personales se expongan a ser robados, por esta razón se hace de suma importancia una evolución jurídica frente a los delitos informáticos y evaluar si realmente está siendo efectiva con el objetivo para el que fueron creadas se hace necesario replantear su definición y adicionar nuevas temáticas para tener un mayor control frente al crecimiento de los delitos

El delito más reportado en Colombia es el hurto por medios informáticos con un total de 31.058 los delincuentes saben que el dinero se encuentra en las cuentas bancarias por eso buscan atacar la interacción entre usuarios y banca el segundo delito más denunciado fue violación a datos personales con 8.037 reportes acceso abusivo a un sistema informático con 7.994 casos las ciudades en las que más se presentaron fue Bogotá Cali y Medellín [4]

[4]lopez, adriana ceballos. 2019-2020. caivirtual. [En línea] 2019-2020. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf. policia. [En línea] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos.

En Colombia se registró el 30% de los ataques rasonware en Latinoamérica las pymes como principal objetivo de los delincuentes pues conocen los bajos niveles de seguridad que manejan las compañías[5]

5.2 OBSERVACIONES REFERENTES A LA NORMATIVIDAD COLOMBIANA A LOS DELITOS INFORMÁTICOS RELACIONADOS CON RED TEAM Y BLUE TEAM

Después de realizar un análisis a los artículos de la ley 1273 de 2009 se propone realizar unas observaciones desde el punto de vista del seminario de especialización y los conocimientos adquiridos ya que para el 2021 se esperan nuevas tecnologías como la inteligencia artificial, BEC basado en deepfake audios y videos de suplantación, botnet para la difusión de correos y el darknet uso de mercados ilegales

Con estas observaciones se pretende generar nuevos artículos y definir cada delito informático y pueda considerarse como base de consulta jurídica y dé claridad sobre cada delito que utiliza medios informáticos brindando más confianza a los ciudadanos

En tiempos de pandemia las transacciones bancarias y la interacción con las redes informáticas aumento, el tele trabajo, los domicilios y las plataformas para el desarrollo de tramites aumento considerablemente, al igual que la tecnología y los grandes cambios que ha generados, esto lleva a que los delincuentes informáticos busquen nuevas formas de engaño y así evadir la normatividad colombiana dejando impune los delitos informáticos

Se recomienda la intervención de las cortes constitucionales internacionales para realizar una investigación a fondo sobre las leyes que regulan los delitos informáticos,

[2]lopez, adriana ceballos. 2019-2020. caivirtual. [En línea] 2019-2020. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf. policia. [En línea] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos.

ARTICULO 269ª ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, utilice equipos, dispositivos o programas para acceder en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.[6]

Modificación. Que utilizando dispositivos o programas para acceder a un sistema informático de forma abusiva y sin ser autorizado o fuera de lo acordado o el solo acceder también será castigado

ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.[7]

Modificación. El que adquiera utilice con conocimiento o de forma empírica intercepte datos informáticos o del espectro electromagnético provenientes de un sistema informático y sin estar facultado en su origen o destino incurre en un delito que puede ser castigado entre 40 y 80 meses de prisión

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.[8]

---

[4]policia. [En línea] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos.

[8] policia. [En línea] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos.

Modificación. El que sin estar facultado realice la instalación de software malicioso o sin licencia que afecte borre suprima o altere datos informáticos incurre en un pena de 50 a 100 meses de prisión

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.[9]

Modificación. El que sin estar facultado para ello trafique adquiera distribuya envié venda extraiga en caso de virus malware, spam, troyanos u otros programas que afecten o dañen o aquellos que no contengan licencias y que causen efectos sobre los dispositivos informáticos incurrirá en una pena de 50 a 100 meses de prisión,

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes

Modificación. El que con objeto ilícito y sin estar facultado, cree perfiles falsos en sitios web, suplante o realice suplantación de identidad mediante el uso de sistemas informáticos o del espectro electromagnético

[9] policia. [En línea] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos.

6 IDENTIFICAR LAS PRINCIPALES FALLAS QUE PUEDE TENER UNA ORGANIZACIÓN EN CUESTIÓN DE SEGURIDAD INFORMÁTICA

Los ciberdelincuentes han evolucionado sus métodos de actuación aprovechándose de las fallas comunes que omiten las empresas o por errores humanos la red se ha convertido en uno de los principales actores de los negocios digitales pero se enfrenta a nuevo retos de ciberseguridad, las redes al igual que otros servicios se encuentra en contante expansión y es difícil proteger ante las amenazas actuales los nuevos dispositivos buscan reducir los riesgos, en muchas ocasiones las fallas de seguridad no se dan , obtener una visión total de los activos y una protección total, una baja complejidad a la hora de configurar y lo más importante la protección contra amenazas el 76 de los expertos en seguridad informática han experimentado la perdida de información en los dos últimos años[10]

La confianza en los equipos de seguridad ha generado a que deleguemos toda las responsabilidad sobre esto, la prevención como es la clave de principal del éxito, en este documento se enmarcan las principales fallas de seguridad que presentan las organizaciones pretendiendo reducir el riesgo de que ocurran

- Contraseñas débiles. A pesar de ser una de las más importantes por lo general es una de las que se le presta menor atención el phishing o suplantación dirigida, los delincuentes mediante el uso de los correos electrónicos convence al usuario para que diligencie sus credenciales en páginas o formularios web estos tiene un punto de convencimiento y persuadiendo al usuario con entidades conocidas.

[10] ¿Conoces las principales razones de las fallas de seguridad de TI? *destinonegocio.com.* [En línea] [Citado el: 12 de 10 de 2020.] https://destinonegocio.com/mx/gestion-mx/razones-de-las-fallas-de-seguridad-ti-2/.

La fuerza bruta también hace parte del robo de contraseñas los delincuentes basados en sus conocimientos inician una serie de comandos buscando la contraseña indicada

- Los wifi gemelos son uno de los más comunes dispositivos utilizados para emitir señales wifi que en el mercado son muy fáciles de conseguir se disfrazan como redes wifi gratuitas estableciendo un señuelo para las personas que mantienen conectadas

- Falta de respaldo informático. En no realizar las copias de seguridad o respaldo inciden siempre en un ciberataque por eso es vital realizar copias de seguridad y así prevenir de una posible pérdida de información. Estas se pueden dar por errores humanos o fallas de equipos de cómputo algo para tener en cuenta es que los datos perdidos no volverán jamás aunque sea posible recuperar desde discos duros las herramientas disponibles en el mercado no son la solución perfecta para recuperar toda la información, los backup existen en tres tipos, completos, incremental diferencial.

- Uso de software pirata. La seguridad informática está directamente relación con la legalidad del software, ya que los programas piratas suelen ser una fuerte amenazas en contra de la integridad de las computadores por eso las empresas ven una disminución en cuanto a ataques informáticos en cuanto toman la decisión de adquirir software de forma legal, de igual manera en el ámbito legal pueden incurrir en sanciones de tipo penal o cierre del establecimiento o monetarias

- Falta de actualizaciones de los sistemas. Las actualizaciones, parches o actualizaciones como uno de los métodos más eficientes de conservar la integridad de la seguridad , un software desactualizado es una potencial amenaza puede llegar a obtener información sensible, confidencias, bases

de datos, cifrar información del servidor o más conocido como ransomware, des configurar los sistemas y asi buscar unos posibles ataques a futuro y por ultimo usar nuestros sistemas para atacar otros, es importante estar actualizado en cuanto a sistemas operativos y estar pendiente de los nuevos parches de seguridad que son actualizados contantemente no sin destacar que algunos sistemas operativos que actualmente está en el mercado no cuentan con soportes es por eso importante migrar a nuevos sistemas operativos para conservar la integridad de nuestra seguridad

- Falta de entrenamiento del personal. La falta de conocimiento por parte del personal al uso de claves es un constante dolor de cabeza para ellos como para los administradores de los sistemas, en la actualidad por parte de un usuario utiliza muchas claves pero todas tiene un parecido y esto lleva a que los delincuentes puedan acceder a mucha información con una sola clave, es de destacar que la frecuencia del cambio también lleva a que usuarios tengan que utilizar claves muy semejantes pare ser recordadas con facilidad otra factor es la frecuencia de uso esto facilita las cosas a la hora de realizar un ataque, por esta razón se hace necesario una buena inducción y una actualización de los manuales de seguridad constantemente

6.1 RECOMENDACIONES AL MOMENTO DE IMPLEMENTAR MEDIDAS DE SEGURIDAD BUSCANDO LA REDUCCION DE INCIDENTES RELACIONADOS CON SEGURIDAD INFORMATICOS

Las empresas depende más de la información en los sistemas, con el paso el tiempo se ha generado un gran valor agregado a dichos activos es por esto que las cada día invierten más recursos en salvaguardar la información de los delincuentes en este documento se busca realizar recomendaciones para mantener la seguridad de las organizaciones por pequeñas que sean

- **El uso de gestores de contraseñas**. Las contraseñas siguen siendo una de las más efectivas formas de contrarrestar la perdida de información usadas para proteger cuentas y programas sim embargo no dejan de ser una brecha de seguridad grande sobre todo por los actores que no dan la debida importancia a cada una de ellas, se recomienda no hacer uso de contraseñas que ya estén utilizadas en otras aplicaciones o programas cambiar de forma contante y lo más importante que las pueda recordar con facilidad, asociarla a canciones direcciones sitios favoritos

- **Administrar las cuentas y los privilegios**. Una buena gestión de cuentas es la clave para evitar incidentes de seguridad informática, para ello se hace necesario controlas las cuentas privilegiadas lo más importantes es reducir estas cuentas al menor número posible, la otra es realizar un inventario de las cuentas que tienes y correctamente registradas por sus categorías es importante analizar las cuentas que se encuentran inactivas y así eliminarlas para dejar la menor.

- Uso de software certificado o legal

  El uso de software legal genera un punto de confianza a la hora de realizar una actualización o buscar una solución a problemas de seguridad, pero un punto para tener principal importancia es que el producto aún se encuentre en el mercado y tenga soporte
- Uso de antivirus, aunque no muchas personas confían en el antivirus siempre es bueno contar como una opción, y tener un buen soporte de este producto puede depender los ataques y detectar los virus

7 RECOMENDACIONES AL MOMENTO DE TENER UN ATAQUE DE SEGURIDAD INFORMÁTICA

Algunos expertos recomiendan no desconectar los equipos de red Cuando se presenta un incidente de seguridad hay que actuar de forma rápida y adecuada en la mayoría de las ocasiones solo sabemos que paso algo cuando un computador presenta fallas o el servidor se apaga pero no nos adelantamos, la documentación de estas fallas es el inicio ideal y tenerlas es de mucho valor para que se desarrollan planes de contingencia, aunque muchos experto en seguridad no lo hace se recomienda realizar con frecuencia la comprobación de backups para verificar que se encuentra en un estado óptimo y pueden prestar su servicio al momento de ser requeridos, en algunas compañías se opta por tener servidores de respaldo y con copias de seguridad almacenadas para estar disponibles en caso de fallas de los principales, en algunos empresas se emplea realizar segmentos de red buscando prevenir y aislar ciertos tipos de redes o equipos y que no interfieran con el desarrollo de las demás actividades otras empresas tomaron la determinación de trabajar a través de un web services y algunas en el uso de certificados digitales.

Se realizan algunas recomendaciones a tener en cuenta al momento de tener un ataque que compromete la seguridad informática.

- Actuar con rapidez para contener el ataque.
- Deshabilitar los archivos que se encuentran infectado
- Desconectarse de la red
- Sistemas de seguridad confiables
- Realización de backup constantes
- Aislar de la red información sensible

8 CONCLUSIONES

Desde el punto de vista analítico este documento busca aportar conocimiento desde el tema legal como el tema cibernético a una norma de seguridad informática como lo son los delitos informáticos, se omite en este caso el apartado de resultados y discusiones y se busca realizar un análisis a los diferentes ataques que pueden ocurrir en el desarrollo de las actividades como expertos en seguridad informática teniendo en cuenta el desarrollo de tecnologías del mercado actual

De igual forma se observan técnicas o herramientas que pueden ser aplicadas para facilitar y endurecer los métodos de seguridad informáticos ya utilizados desarrollo y mejorar las capacidades de reacción al momento de que ocurra un ataque informático.

9 BIBLIOGRAFIA

Ceballos Adriana, gracia bautista Fredy, meza guzmán Lorena, quintero Carlos. Tendencias cibercrimen Colombia 2019-2020. [En línea]. Disponible en https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Delitos informáticos y entorno jurídico vigente en Colombia [en línea] disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Marrugo Jimenes Ivan Dario .Colombia y la cooperación internacional en los delitos informáticos [en línea] disponible en https://www.ambitojuridico.com/noticias/educacion-y-cultura/colombia-y-la-cooperacion-internacional-en-los-delitos-informaticos

Nmap, [En línea]. Disponible en: https://www.ecured.cu/Nmap

Cárdenas Gómez Roberto La herramienta nmap [En línea], disponible en: http://www.cryptomex.org/SlidesSeguridad/nmap.pdf

A Esaú. Nmap, uso básico para rastreo de puertos [En línea], Disponible en:https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/#:~:text=Nmap%20es%20uno%20de%20los,funci%C3%B3n%20como%20veremos%20a%20continuaci%C3%B3n.

Lyon Gordon Técnicas de sondeo de puertos [En línea], disponible en: https://nmap.org/man/es/man-port-scanning-techniques.html

Jiménez Tandazo Karla, Rueda Salgado Miguel Angle Prevención, Detección y Reducción de riesgo de ataques por escaneo de puertos usando tecnologías de virtualización [En línea], disponible en:https://repositorio.espe.edu.ec/bitstream/21000/6906/1/T-ESPE-047328.pdf

Yaguez Rios Javier Técnica y herramientas de análisis de vulnerabilidades de una red [En línea], disponible en: http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf

Barbleri Leonardo kasperskt registra 45 ataques por segundo en america latina [En línea], disponible en:https://www.itwarelatam.com/2019/08/28/kaspersky-registra-45-ataques-por-segundo-en-america-latina/

Poggi Nicolas, 24 estadísticas de seguridad informática que importan en el 2019 [en línea], disponible en:https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

nn. tests de intrusión y explotación de vulnerabilidades: uso básico de mestasploit [en línea], Disponible en:https://ccia.esei.uvigo.es/docencia/ssi/1819/practicas/ejercicio-metasploit/

catoira fernando, pruebas de penetración para principiantes: explotando una vulnerabilidad con metasploit framework [en línea] disponible en:https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%c3%b3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Romero castro marta Irene , Figueroa moran Liliana, vera Navarrete Denisse Soraya, Álava Cruzatty Jose Efrain, parrales Anzules galo Roberto, Alava mera Cristian José, murillo Quimiz Qngel Leonardo, castillo merino Mirian Adriana, Introducción a la seguridad y el análisis de las vulnerabilidades [en línea] Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Tipología de proyectos calificación como de carácter científico tecnológico e innovación, versión 5 [En línea] Disponible en:https://minciencias.gov.co/sites/default/files/upload/convocatoria/anexo_3._documento_de_tipologia_de_proyectos_version_5_1.pdf

Harán juan Manuel, advierten sobre los riesgos de seguridad que supone seguir utilizando windows 7[en línea] disponible en: https://www.welivesecurity.com/la-es/2020/08/06/advierten-sobre-los-riesgos-de-seguridad-que-supone-seguir-utilizando-windows-7/

¿Conoces las principales razones de las fallas de seguridad de TI? *destinonegocio.com.* [En línea].Disponible en.:https://destinonegocio.com/mx/gestion-mx/razones-de-las-fallas-de-seguridad-ti-2/.

lopez, adriana ceballos. 2019-2020. caivirtual. [En línea]Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf.

policia. [En línea] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos.

Biscontini T. Computer Security. Salem Press Encyclopedia of Science [en línea] Disponible en.http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=ers&AN=87321231&lang=es&site=eds-live&scope=site