ETAPA 5

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

CARLOS ANDRES VARGAS RODRIGUEZ

UNIVERSDIAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA PLATA HUILA
2020

ETAPA 5

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

CARLOS ANDRES VARGAS RODRIGUEZ

Guía de actividades - Etapa 5 – Socialización de Informe Técnico

JOHN FREDDY QUINTERO TAMAYO
M.Sc.

UNIVERSDIAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA PLATA HUILA
2020

CONTENIDO

1. RESUMEN

El siguiente informe es el resultado del proceso de aprendizaje, que se logra a través del estudio de los contenidos y las prácticas propuestas, para el desarrollo del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Read Team & Blue Team, mediante la estrategia ABP (Aprendizaje Basado en Problemas), abordado en tres unidades temáticas. La Primera Unidad hace referencia al contexto legal y ético que se deben tener presentes y ser aplicados por los integrantes de los Read Team o Blue Team, cuando ejecutan sus labores de ciberseguridad diarias. La Segunda Unidad denominada Pasos y Procesos Read Team, que enmarca todas las estrategias y herramientas que sirven de apoyo a la hora de identificar los fallos de seguridad, que se presentan en las plataformas o en cualquier sistema de información y La Tercera Unidad llamada Análisis y Contención en Blue Team, que abarca todos los procesos y herramientas que se pueden utilizar tanto para evitar o contener ataques informáticos, como para reparar dichos sistemas, generando con ello el uso de buenas prácticas para la seguridad de un sistema informático dentro de una empresa u organización.

2. GLOSARIO

HARDENING: palabra que en ingles significa endurecimiento. Con respecto al área de informática se dice que es el proceso de asegurar un sistema, mediante la reducción de vulnerabilidades en el mismo.

SIEM: (información de seguridad y gestión de eventos). Tecnología capaz de detectar rápidamente, responder y neutralizar amenazas informáticas.

SMBv1: Protocolo de red para compartir recursos.

CVE-2017-0144: Código vulnerabilidad detectada en sistemas operativos Windows aplicada en el protocolo SMBv1.

MS17-010: Código para identificar actualización se SO Windows aplicada el 14 de marzo de 2017.

PENTESTING: Son las prácticas que se realizan para atacar a un sistema informático, con el fin de encontrar fallos en el mismo.

3. OBJETIVO GENERAL

Lograr el desarrollo de habilidades, que permitan planificar, ejecutar y solucionar problemas, eventos, incidentes o ataques de ciberseguridad informática a un sistema o infraestructura TI, teniendo en cuenta siempre el código de ética y las leyes que rigen en este tema para no cometer delitos informáticos.

4. OBJETIVOS ESPECIFICOS

- Crear grupos especializados para el manejo de la seguridad de un sistema informático, garantizando con ello la protección permanente del sistema.
- Desarrollar el uso de métodos o técnicas de intrusión para generar situaciones de ataque informático, con el fin de determinar las vulnerabilidades que presente un sistema informático.
- Identificar con claridad todos los procesos que se deben llevar a cabo, para proteger o robustecer la seguridad de un sistema informático.
- Identificar de manera rápida y ágil, aquellas acciones que generen indicios de un ataque informático.
- Planear estrategias, que permitan contener ataques informáticos.
- Proponer soluciones concretas para contener de manera inmediata un ataque informático, bien sea cuando el sistema este activo o inactivo.
- Identificar todas aquellas herramientas (software, hardware), que permitan contribuir a una mayor seguridad del sistema.
- Crear, mantener y actualizar el desarrollo de buenas prácticas de ciberseguridad, para fortalecer los sistemas informáticos.
- Conocer las leyes, que rigen en todo el territorio nacional sobre todas aquellas acciones que son consideradas como delitos informáticos, con la finalidad de no incurrir en ellas a la hora de ejecutar procesos que puedan vulnerar la seguridad de un sistema informático y vulnerar la integridad de las personas que resulten implicadas en estos asuntos.

5. INTRODUCCION

La creación de Equipos Estratégicos de Ciberseguridad (Read Team & Blue Team), surgen de la necesidad de proteger los sistemas de información, que a diario son atacados con distintas finalidades y en la mayoría de los casos con fines oscuros o criminales. Estos equipos tienen como misión, el desarrollar habilidades que les permitan planificar, ejecutar y solucionar todos aquellos problemas que se generen por un ataque informático. Para lograrlo deben encaminar todos sus conocimientos y seguir una hoja de ruta que les permita cumplir con los objetivos propuestos. Es por ello que este seminario abarca los principales temas que se deben tener en cuenta, para guiar las labores o procesos, que se deben dar dentro esta clase de equipos, con el fin de orientarlos y permitir que se cumplan con los objetivos propuestos. A continuación se expone el desarrollo de todas las actividades propuestas en este seminario.

6. DESARROLLO DEL INFORME

Con respecto a la **Unidad 1**, Contexto Ético, Legal Read Team & Blue Team, se llevaron a cabo tres procesos, por una parte las lecturas indicadas para esta unidad, suministradas por el tutor; por otra las búsquedas realizadas a través de internet para ampliar la información con respecto de la leyes que existen en Colombia, con el fin de identificar las acciones que son tipificadas como delitos informáticos, el tema de las pruebas de penetración o pentesting, las herramientas utilizadas para este tipo de pruebas y finalmente la configuración del Banco de Trabajo, para la realización de la parte práctica de esta unidad. De las anteriores consultas y lecturas se obtuvo la siguiente información:

NORMATIVIDAD SOBRE DELITOS INFORMATICOS:

Ley 1273 de 2009: "De la protección de la información y de los datos: cuya característica principal es preservar los sistemas que usan tecnologías de información y comunicaciones, así mismo quien incurra en estos delitos y en virtud al código penal colombiano tendrá penas de prisión y multas, otros delitos que se encierran en ésta ley y que también son penalizados son: Atentar en contra de la confidencialidad de las empresas, el acceso abusivo, la obstaculización del normal funcionamiento del sistema, la intercepción de datos informáticos, la suplantación de sitios web para hurtar información personal, transferir activos sin consentimiento"[1].

[1] LEY 1273 DE 2009. Formato PDF. {En línea} {08 de septiembre de 2020} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009. pdf).

Ley 1581 año 2012: Caracterizada por clasificar y proteger los datos personales, en donde se define como dato personal de acuerdo a le ley 1581 (2012); “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas”.

Documento CONPES 3854, 11 de abril de 2016: Sobre la política nacional de seguridad digital, cuyas características son la protección de las entidades estatales contra posibles ataques cibernéticos y la prevención de los mismos.

Decreto 1377 de 2013: Es un decreto para reglamentar la ley 1581 de 2012, se caracteriza por la protección de datos personales, tocando temas relacionados a la transferencia y transmisión de datos, el tratamiento de los datos, seguridad de la información en las organizaciones.

Ley 1712 de 2014: Transparencia y del Derecho de Acceso a la Información Pública y Nacional, se caracteriza por contar con unos principios que son de publicidad, transparencia, buena fe, facilitación, discriminación, gratuidad, celeridad, eficacia, calidad de la información, divulgación de la información, responsabilidad en el uso de la información, esta ley permite el derecho al acceso de la información pública publicada en los sistemas de información del estado”.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la ley 1712 de 2014; se caracteriza por tener consideraciones en cuanto al derecho de la

información pública y la protección de la misma, otra característica es que dicha información está a cargo de la secretaria de transparencia de la presidencia, del ministerio de tecnologías de la información y comunicaciones, entre otros, Así mismo; Dicha información se clasifica, se reserva, se publica y divulga adecuadamente.

PRUEBAS DE PENETRACION O PENTESTING

Son las prácticas que se realizan para atacar a un sistema informático, con el fin de encontrar fallos en el mismo.

ETAPAS DEL PENTESTING:

"Reconocimiento: En esta etapa se busca toda la información de la empresa o entidad que sea de utilidad para poder ingresar al sistema, algunas de las herramientas útiles serían los buscadores como Google y algunas redes sociales que nos proporcionen información relevante de la misma como Facebook e Instagram.

Escaneo de puertos, servicios, OS: En esta etapa se pretende conocer muy bien el sistema que queremos atacar, para lo cual se ejecuta un escaneo cuya finalidad sea encontrar los host activos en la red con mucha discreción y de la manera menos tediosa posible; Una herramienta de gran utilidad sería Nmap que se usaría para explorar la red.

Identificación de sistemas, puertos activos, servicios y usuarios: La idea en esta etapa es realizar una identificación plena del sistema operativo, de los potenciales blancos en el sistema, de modems, de configuraciones inseguras, entre

otros, con el objeto de realizar una exploración de las posibles entradas al sistema, para esto se hace uso de herramientas como Nmap

Análisis de vulnerabilidades: El objetivo de la presente etapa es encontrar fallas en el sistema, por medio de las cuales podamos acceder más fácilmente a él, para ello se puede utilizar herramientas como: Nessus.

Explotación de vulnerabilidades: Es aprovechar al máximo la vulnerabilidad detectada con antelación a fin de acceder al sistema, una herramienta utilizada puede ser Metasploit.

Informes: Aquí se documenta todo el proceso detallando cómo se llevó a cabo la intrusión al sistema y qué herramientas se utilizaron en cada una de las etapas. Las herramientas que se usan en esta etapa deben ser formatos de fácil comprensión como por ejemplo SSL".[2]

HERRAMIENTAS UTILIZADAS PARA PRUEBAS DE PENETRACION O PENTESTING :

• "**Metasploit"[3]:** Es una herramienta utilizada en las pruebas de penetración o pentesting, es completa, gratuita y multiplataforma para la protección de datos y la seguridad informática, está dirigida a auditores de seguridad y equipos Red team y blue team, quienes se encargan de detectar las vulnerabilidades de los sistemas y de la prevención de ataques informáticos, esta herramienta consta de bastantes

[2] GUILLÉN ZAFRA, José Luis. "Introducción al pentesting". Barcelona, 2017. 66p. {En línea} {30 de septiembre de 2020} disponible en (http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf)

[3] REVITA SEGURIDAD. CATORIA, Fernando. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. {En línea} {08 de septiembre de 2020}. Disponible en: (https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra)

vulnerabilidades ya conocidas y es útil para la evasión de sistemas de seguridad, se caracteriza por tener la capacidad de interactuar con otras herramientas, de importar y exportar datos.

• **Nmap:** Es una herramienta gratuita y multiplataforma, útil para rastrear puertos, explorar la red, identificar sistemas informáticos y evaluar sus ventajas, se caracteriza por su flexibilidad, por identificar puertos abiertos, sistema operativo y la versión que utiliza un host determinado, se puede usar en redes de gran tamaño, es portable gracias a que se puede utilizar en cualquier sistema operativo, su sintaxis es sencilla razón por la que facilita su uso.

• **OpenVas:** Esta herramienta multiplataforma utilizada para escanear y buscar vulnerabilidades de seguridad en un sistema informático "apoyándose en una base de datos" tal como lo indica Guillén, José (2017)[2], se caracteriza por posibilitar el escaneo de varios hosts simultáneamente, tiene la capacidad de emitir sus reportes en múltiples formatos.

Servicios en línea:

• **ExploitDB:** Este servicio sirve para beneficiarse de una vulnerabilidad de un sistema de información, un exploitDB es una herramienta para aprovechar un fallo de seguridad, cuyo objetivo radica en lograr acceso administrativo a un equipo."

• **CVE:** Common Vulnerabilities and Exposures , Es un identificador que utilizan las herramientas de ciberseguridad, dicho identificador o código se le asigna a la vulnerabilidad encontrada, que Según Martí, Rafael (2016); "Son referencias para identificar una vulnerabilidad concreta, es útil para ampliar información en bases de datos"[4], usa un formato CVE - El año de descubrimiento de la vulnerabilidad - El número de la

vulnerabilidad, por ejemplo: CVE-2020-1354. Su utilidad radica en que se puede acceder al CVE fácilmente, además se puede usar para buscar problemas en la base de datos de las vulnerabilidades.

CONFIGURACION DEL BANCO DE TRABAJO

Para la configuración del banco de trabajo se realizaron las indicaciones dadas de la siguiente forma:

Figura No. 1 Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

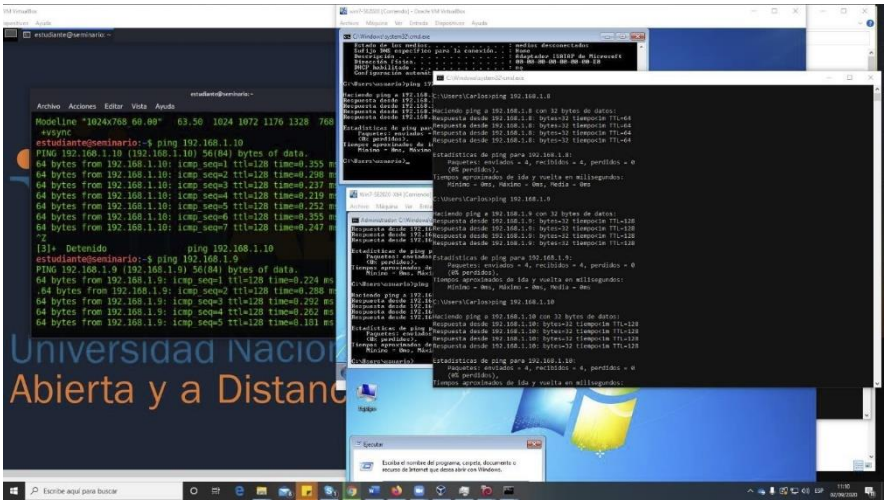
Fuente: Autor

• Descargar herramientas requeridas para realizar el montaje del banco de trabajo, como las imágenes en formato OVA, las cuales ya están pre-configuradas para ser utilizadas en las actividades de carácter técnico. En las imágenes OVA existe: Un Windows 7 X86, un Windows 7 X64, un Kali Linux.

Figura No. 2 Corresponde a las máquinas virtuales instaladas en virtual box, identificando en banco de trabajo para las practicas.

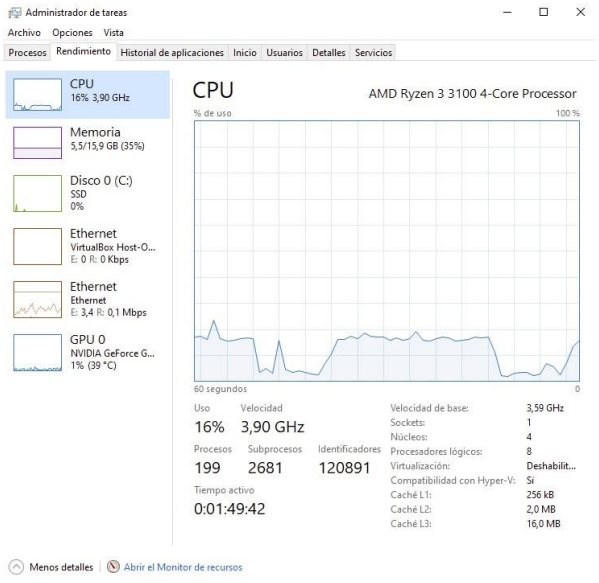
Fuente: Autor

Figura No. 3 Corresponde la ejecución de las 3 máquinas virtuales y su respectivo ping de conexión.



Fuente: Autor

Figura No. 4 Se Evidencia con printscreen el montaje del banco de trabajo y se explica cómo se encuentra desplegado “características técnicas de hardware”.



Fuente: Autor

Maquina Anfitrión

Procesador Ryzen 3 3100 4 núcleos 8 subprocesos

16 RAM 8x2 a 3200 Mhz

SSD 1 TB Crucial

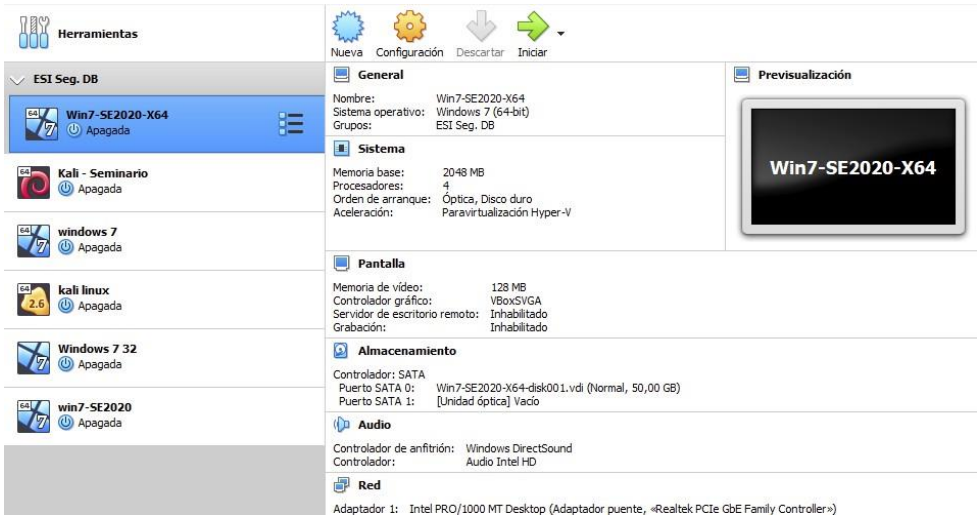
Board B450

TUF GAMING

GPU GTX

1650 SUPER

Figura No. 5 Se depliage la configuration de la máquina virtual con windows 7 64 bits

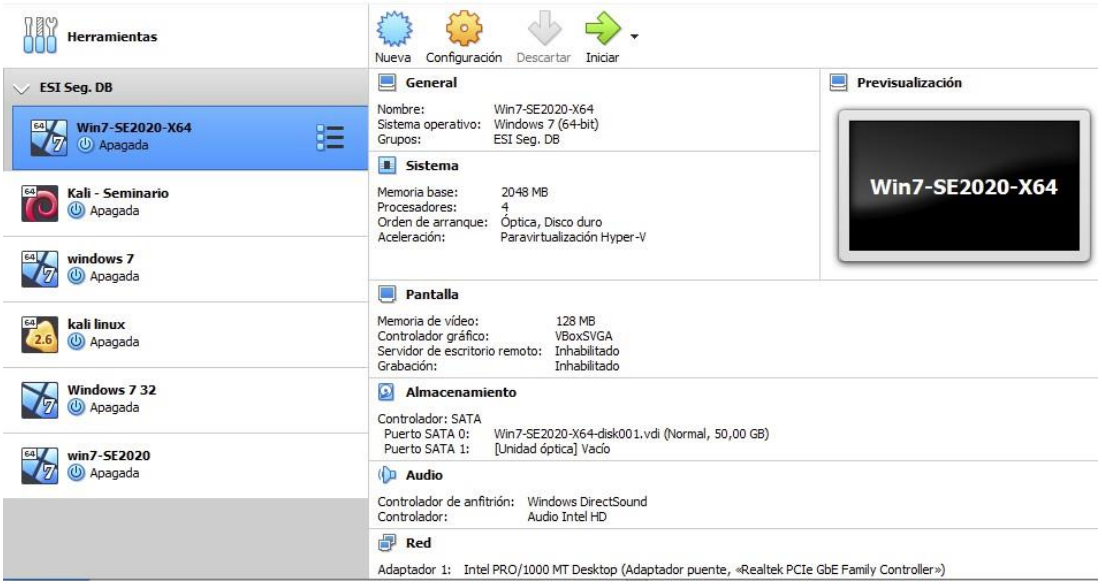


Fuente: Autor

Las máquinas virtuales están todas configuradas de la siguiente forma:

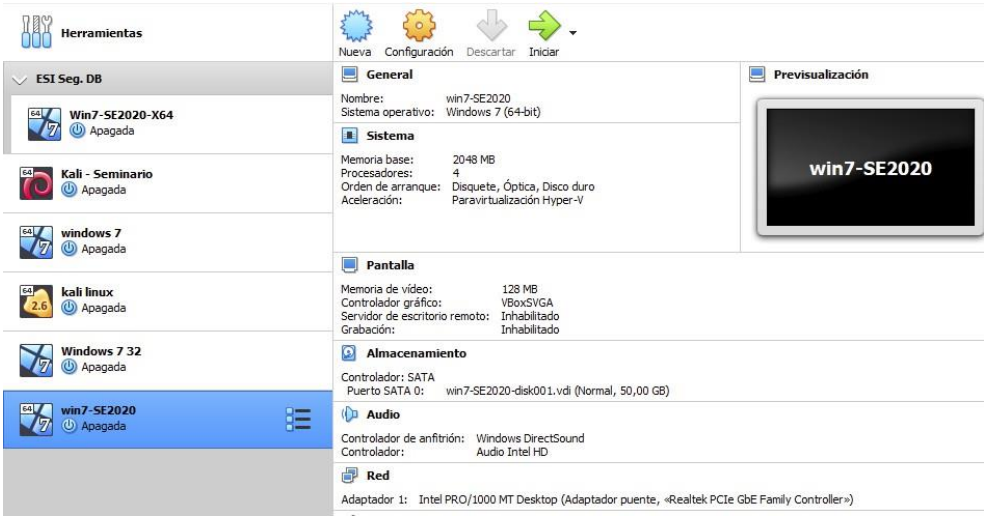
Se compartió 4 núcleos del procesador, 2 GB de RAM y 128 MB de video, esto con el fin de poder ejecutar las 3 máquinas al tiempo y hacer las pruebas pertinentes.

Figura No. 6 Configuración máquina Kali Linux



Fuente: Autor

Figura No. 7 Configuración Windows 7 32 bits



Fuente: Autor

Con relación a la **Unidad 2**, Pasos y Procesos Read Team & Blue Team, se desarrollaron tres actividades. La primera encaminada a identificar en el Acuerdo de confidencialidad para la contratación de los equipos Read Team & Blue Team, la presencia de procesos ilegales y no éticos dentro del acuerdo. Además de realizar un análisis detallado sobre el caso Operación Andromeda Buggly, finalizando el trabajo de esta unidad con el desarrollo de la actividad práctica, en la que se aplicaron distintas herramientas, para evaluar la vulnerabilidad del sistema y de esa forma encontrar el método para lograr penetrar en el sistema. El desarrollo de esta unidad se ejecuta como sigue:

Una vez identificadas las leyes que tipifican los delitos informáticos, se procede al análisis detallado del acuerdo de confidencialidad establecido entre la organización White House Security y el posible estudiante para hacer parte del equipo Read Team & Blue Team, se logra evidenciar que existen falencias dentro del acuerdo, que conllevan a ejecutar de muchas maneras procesos que generan acciones de carácter ilícito, incurriendo en delitos y vulnerando la integridad y privacidad de todos aquellos que han confiado en la organización White House Security. Además de ello es en esta parte de la contratación donde priman también, los principios y valores éticos que como profesionales se deben tener en cuenta, a la hora de ejecutar la profesión, porque si bien es cierto que se recibe una remuneración por el trabajo realizado, este se debe ejecutar de manera correcta, clara y legal para no generar afectaciones delictivas. A continuación se enuncian las cláusulas del acuerdo, que pueden estar violando las leyes y el código de ética que rige para los Ingenieros.

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

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial."

Cuarta. Obligaciones de la parte receptora incisos:

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

"7. Responder por el mal uso que le den sus representantes a la información confidencial."

"9. 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 parte de Whitehouse Security.""[4]

Apreciaciones:

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

[4] ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA, Anexo 3, Acuerdo.

Security no podrán ser divulgados." Llama la atención que de entrada en la cláusula mencionada, aparece el término "procesos ilegales", lo que conlleva a pensar que si se realizan procesos poco convencionales para realizar el trabajo.

Con respecto a la cláusula tercera, origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial." Pareciera ser una clausula clara acerca de donde proviene la información, pero esta cláusula no hace mención a la forma o a los procesos específicos que se hacen para poder obtener esa información y es ahí en donde se puede incurrir en las faltas que las Leyes Colombianas tipifican como delitos.

Con respecto a la cláusula cuarta, obligaciones de la parte receptora, inciso 7, "responder por el mal uso que le den sus representantes a la información confidencial", me genera gran inquietud, pues si bien es cierto que a la hora de firmar un contrato se acepta todo lo que en él está contenido, es una cláusula para tenerla en cuenta y analizarla muy detalladamente y lo que implica; pues al presentarse problemas de tipo ilegal, la responsabilidad también recae sobre el empleado y las consecuencias que se pueden originar de una situación como esta sería la detención y privación de la libertad por el tiempo que así lo considere la justicia y de acuerdo a la falta cometida, fuera de ello se puede perder el derecho a ejercer su profesión o bien por un periodo de tiempo o no volver a ejercer la

profesión, seguido de todos los problemas de carácter familiar y social que acarrean situaciones como las antes mencionadas.

Con respecto a la cláusula cuarta, obligaciones de la parte receptora, inciso 3, no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros, es de tener muy presente, pues en muchas ocasiones este tipo de actividades está asociado a hechos delictivos como extorsiones, secuestros y asesinatos entre otros y el no denunciarlos implica que se es cómplice de estos actos ilícitos.

Con respecto a la cláusula cuarta, obligaciones de la parte receptora, inciso 9, 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 parte de Whitehouse Security." En esta cláusula claramente se habla de información confidencial o "**ilegal"** por lo tanto la organización si es conocedora y acepta que incurren en procesos ilegales cuando así lo requieren.

Al evidenciar que en el acuerdo se estipulan procesos ilegales y no éticos, se mencionan los artículos de la ley 1273, que se vulneran en el acuerdo:

"Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Para obtener la información que desean se aprovechan de la vulnerabilidad en el acceso a los sistemas de información.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS: Cuando se ingresa sin orden judicial previa, para interceptar datos informáticos en su origen, destino, o en el interior de un sistema informático.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES: Cuando sin estar facultados se crean páginas similares a las de una entidad y se envían correos, spam, ofertas de empleo y de esa manera las personas suministran información de tipo muy personal.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes".[5]

En este punto se genera el siguiente interrogante: ¿Existiendo procesos poco confiables acuerdo? Usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

No aplicaría para este trabajo, pues en el acuerdo propuesto hay cláusulas que no especifican de manera concreta y detallada, la forma como se deben realizar los procesos para el caso de obtener información, generándome desconfianza puesto que sé, que en algún momento se puede incurrir o estar tipificados en los delitos que la ley considera como atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de información, consignados en la Ley 1273 de 2009. Por otra parte cabe resaltar que la toma de esta decisión también está influenciada por los principios éticos, para nuestro caso los enmarcados en el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares; en el cual se encuentran el catálogo de conductas profesionales, que se exigen, se prohíben o que inhabilitan a los ingenieros en general y a sus

[5] LEY 1273 DE 2009. Formato PDF. {En línea} {08 de septiembre de 2020} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

profesionales afines o auxiliares. Algunos de los deberes importantes y a tener en cuentan están:

“ARTICULO 31. DEBERES GENERALES DE LOS PROFESIONALES

Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.

Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones.

Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.

ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES.

Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.

Velar por el buen prestigio de estas profesiones.

ARTÍCULO 37. DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.

Abstenerse de emitir públicamente juicios adversos sobre la actuación de algún colega, señalando errores profesionales en que presuntamente haya incurrido, a no ser de que ello sea indispensable por razones ineludibles de interés general o, que se le haya dado anteriormente la posibilidad de reconocer y rectificar aquellas actuaciones y errores, haciendo dicho profesional caso omiso de ello.

Obrar con la mayor prudencia y diligencia cuando se emitan conceptos sobre las actuaciones de los demás profesionales.

ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL".[6]

Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.

Dedicar toda su aptitud y atender con la mayor diligencia y probidad, los asuntos encargados por su cliente.

Los profesionales que dirijan el cumplimiento de contratos entre sus clientes y terceras personas, son ante todo asesores y guardianes de los intereses de sus clientes y en ningún caso, les es lícito actuar en perjuicio de aquellos terceros.

---

[6] CONSEJO PROFESIONAL NACIONAL DE INGENIERA COPNIA. República de Colombia. Código de ética para el ejercicio de la Ingeniera en general y sus profesiones afines y auxiliares. {En línea} {07 de septiembre de 2020} disponible en: (https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica).

Es probable que para otros resulte llamativa y tentadora la oferta de tener un “contrato vitalicio” y que la cantidad ofrecida también les parezca suficiente para aceptar la oferta. Pero vale la pena estudiar a fondo y con calma, cada una de las cláusulas que componen un contrato de trabajo, analizando todas las situaciones que se pudieran presentar en un futuro y cuáles podrían ser las posibles consecuencias, ante situaciones complejas y como afecta al contratado. Desafortunadamente convivimos en un mundo en donde muchas veces priman por sobre todas las cosas los intereses económicos, sin importar a que costo y se olvidan los valores y principios éticos, que como personas se deben tener presentes a la hora de actuar de manera correcta. Siempre tendrá más valor, aquel que trabaja con honestidad y rectitud, que a aquel que se vale de artimañas para lograr lo que se propone y pueda que mantenga una cuenta bancaria con suficientes fondos, pero sin tranquilidad y con la zozobra de no saber a qué horas se puede derrumbar aquello que creyó construir.

Una vez aplicado el marco legal y el código de ética para ingenieros, al acuerdo de confidencial expuesto en el anexo 3, se hace un resumen general del caso “OPERACIÓN ANDROMEDA BUGGLY” enmarcando las implicaciones legales y éticas que se pudieron generar. Por lo tanto el resultado obtenido luego del proceso de investigación y lecturas es el siguiente:

A mi entender y de acuerdo a lo leído sobre el tema, expreso lo siguiente: “Buggly fue un hackerspace (Lugar en el cual personas ingeniosas, cooperativas y con ganas de aprender, se reúnen a compartir información relevante sobre todo lo que hacen y cuyo objetivo principal es aprender unos de otros, sobresaliendo entre ellos la colaboración) siendo el objetivo principal de este lugar el de construir una comunidad de seguridad informática y así lo hizo parecer. Pero como siempre hay quien coloque el dedo en la llaga, surgieron dudas sobre los dineros para soportar o financiar este tipo de proyecto y más cuando en el lugar se ofrecían todo tipo de comodidades para ingresar en él y sin complicaciones. Resulto ser que Buggly no

era el lugar ingenuo, puro, sencillo que muchos creían que era. Aparentemente en Buggly se llevaba a cabo la Operación Andrómeda, una fachada de la Central de Inteligencia Técnica del Ejercito Nacional y cuyo objetivo era el de adquirir conocimiento de informática sobre el hacking ético (Forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin ocasionar daños.) el lugar aparte de ser frecuentado por personas del común también era visitado por militares o empleados de las Fuerzas Armadas. Se dice que desde Buggly se realizaban monitores del espectro; se utilizaban los llamados malware para obtener información de personas, conllevando a la interceptación de comunicaciones; usaban software especiales para espiar computadores teniendo por lo tanto control absoluto sobre todo el manejo de la información tanto de entrada como salida y que este método era el utilizado para espiar a las guerrillas de las FARC y el ELN. También se dice que desde Buggly se hacía espionaje al proceso de paz. La fachada de Buggly según el General Ernesto Maldonado era legal, fundamentada en la Constitución Política de Colombia, directivas, reglamentos y el Manual de Manejo de Redes e Informantes. Según parece no había un control adecuado sobre las actividades que se realizaban tanto por parte del personal militar como del personal civil y trabajaban sin ningún tipo de supervisión. Al final los señores encargados del manejo de Buggly, rompen con sus propios códigos de ética, tal vez cegados por la ambición de poder y ambición al dinero y terminan vendiendo la información obtenida en Andrómeda a terceras personas, con fines lucrativos sin importar el daño y caos que pudieran generar; los rumores siguieron creciendo y finalmente se destapa la olla, como decimos coloquialmente cuando se afirma que desde Buggly se estaba haciendo espionaje al proceso de paz. Luego de ser descubierta dicha actividad ilícita, los implicados terminan aceptando que efectivamente si hubo malos manejos en los procesos que allí se llevaban a cabo, lo que conlleva a la investigación por parte de los órganos establecidos para ello, de todos los que estaban involucrados, determinando las sanciones, castigos o penas de acuerdo a Ley Colombiana, por lo que hubo

destituciones, exclusiones y retiros del servicio activo, como los procesos de investigación para determinar las penas a pagar por estos delitos".[7]

De acuerdo a lo anterior las implicaciones legales de los delitos cometidos, en este caso corresponden a: **Acceso abusivo a un sistema informático**, el cual será sancionado con una pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes; **Interceptación de datos informáticos,** será sancionado con una pena de prisión de 36 a 72 meses; **Uso de Software malicioso,** será sancionado con una pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes; **Violación de datos personales,** será sancionado con una pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes; **Espionaje,** incurrirá en prisión de 64 a 216 meses.

Con respecto a las implicaciones éticas y lo consignado en el Código de Ética para El Ejercicio de la Ingeniera, se puede hacer efectiva la suspensión la matricula profesional por un periodo de 5 años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios y la cancelación de la Matrícula Profesional, cuando las faltas cometidas son gravísimas.

Finalmente se lleva a cabo desarrollo de la actividad práctica, en la que se aplicaron distintas herramientas, para evaluar la vulnerabilidad del sistema y de esa forma encontrar el método para lograr penetrar en el sistema de la siguiente forma:

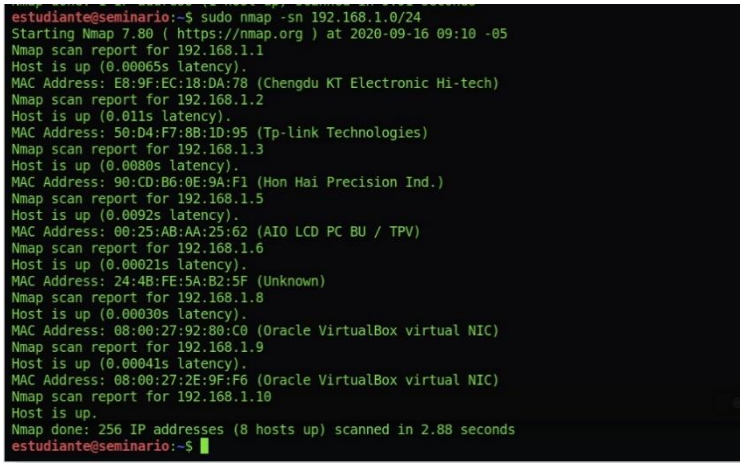
[7] ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. {En línea} {09 de septiembre de 2020} disponible en: (https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/).

HERRAMIENTAS PARA ESCANEO DE EQUIPOS EN LA RED

Para buscar los equipos en la red, se utilizó Nmap en Kali Linux para hacer un escaneo, con el siguiente comando

-nmap -sn 192.168.1.0/24

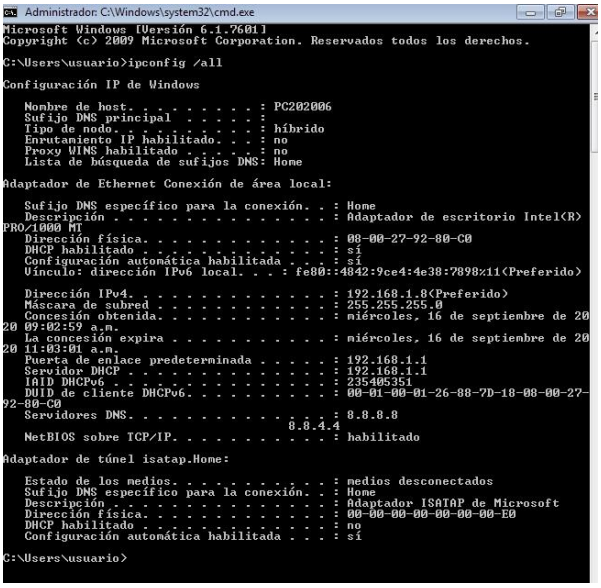
Figura No. 8 resultado del comando nmap:



Fuente: Autor

Se encuentra varias máquinas conectadas, puerta de enlace, modem tp-link donde se comparte la red a otros dispositivos, pero lo más importante son las ip: 192.168.1.8 y 192.168.1.9. Corresponde a las maquinas analizar y encontrar sus posibles problemas de seguridad.

Figura No. 9 Equipo 192.168.1.8 máquina virtual con Windows 7 64 bits



Fuente: Autor

Figura No. 10 Equipo 192.168.1.9 máquina virtual con Windows 7 32 bits

Fuente: Autor

HERRAMIENTAS PARA LA IDENTIFICACIÓN DE SISTEMAS, PUERTOS ACTIVOS, SERVICIOS Y USUARIOS

"El comando**- Nmap-O (Dirección IP)** permite conocer puertos abiertos e identificador del sistema operativo. Una vez que se tiene acceso a las máquinas virtuales y se identifican los sistemas operativos, se revisan los puertos abiertos. Es parte importante la identificación de los puertos abiertos, en la fase de conocimiento, son puertas abiertas donde puede elaborar un plan de análisis".[8]

HERRAMIENTAS PARA IDENTIFICAR VULNERABILIDADES DEL SISTEMA

Para encontrar vulnerabilidades se usa la herramienta NESSUS, que permite escanear la red y encontrar software con exploits, identificación de sistemas. Como en la maquina Kali Linux no se encuentra el programa se procede hacer la respectiva instalación, un vez instalado se procede a iniciar el servicio y se ejecuta el análisis a las dos máquinas, para revisar todas las vulnerabilidades que tiene y también identificar que efectivamente contiene la perdida de información por SMBv1: Protocolo de red para compartir recursos y el CVE-2017-0144: Código vulnerabilidad detectada en sistemas operativos Windows aplicada en el protocolo SMBv1. Arrojando como resultado que para el sistema operativo Windows 7 home 32 bits se encontraron 25 vulnerabilidades, y para el sistema Windows 7 profesional 64 bits con 21 vulnerabilidades. Una vez detectadas las vulnerabilidades del sistema, se procede a la utilización de herramientas como el exploit que permitirán acceder a las vulnerabilidades del sistema y poder acceder a los archivos a los que se quieren acceder. Las evidencias de la parte práctica sobre el tema que se está tratando están expuestas en el video que para ello se llevó a

[8] BYTE MIND. Escaneando la Red con Nmap en Kali Linux. {En línea} {09 de septiembre de 2020} disponible en: https://byte-mind.net/escaneando-la-red-con-nmap/).

cabo y que se adjunta para hacer un recuento paso a paso del desarrollo de la actividad práctica y entender de manera más práctica lo consignado en teoría.

Para el desarrollo de las actividades propuestas en la **Unidad 3**, Análisis y Contención en Blue Team, se realizan las lecturas correspondientes para esta unidad y que comprende los temas de Contención de ataques; Hardening; Sistema SIEM (Información de seguridad y Gestión de Eventos); Herramientas Software y Hardware para la Contención de Ataques; además de las consultas realizadas en la Web para profundizar los temas, se finaliza el proceso de aprendizaje de esta unidad llevando a la práctica, el desarrollo de actividades que minimicen las vulnerabilidades del sistema y evitar de esta manera posibles ataques informáticos.

HARDENING

"Conjunto de procesos, actividades u acciones que son realizadas o ejecutadas por el administrador del sistema operativo, con el fin de robustecer al extremo la seguridad de los equipos de informática. La finalidad del Hardening es evitar que se lleve a cabo un ataque y actuar de manera rápida y efectiva para frenarlo y así salvaguardar la información o los datos que se manejan.

PRACTICAS DE HARDENING:

Verificar todas las configuraciones relacionadas con la seguridad del equipo, para comprobar su debida activación y en caso de no estarlo corregir la situación.

Verificar las configuraciones y activaciones de las actualizaciones automáticas.

Verificar si hay instalados programas de seguridad, entre ellos antivirus, antispyware o antispam.

Verificar todas las claves que se manejen dentro del equipo para determinar si son las correctas o de lo contrario proceder a cambiarlas por claves más complejas.

Verificar el manejo de todos los programas que se encuentren instalados en el equipo, determinando el uso y quien los maneja.

Verificar las configuraciones relacionadas con la acción Acceso Remoto, limitando su uso y la cantidad de usuarios que pueden ejecutar esta acción.

Verificar las configuraciones relacionadas con las cuentas de los usuarios.

Verificar las configuraciones relacionadas con los backup, con el fin de que se hagan copias de seguridad.

Verificar la configuración de la red.

Verificar si el sistema cuenta con aplicaciones específicas que permitan monitorear la red.

Verificar si el sistema cuenta con implementación de auditorías.

Verificar si el sistema cuenta con un sistema de detección de intrusos.

Verificar la configuración de Firewall.

Verificar que el sistema operativo ha sido instalado de manera segura y correcta".[9]

SISTEMA SIEM (Información de Seguridad y Gestión de Eventos)

Tecnología del tipo software que puede detectar, responder y contrarrestar o neutralizar amenazas informáticas de manera muy rápida. Su objetivo principal y de acuerdo a su concepto es la evitar y frenar a toda costa que los sistemas

[9] HACKERUNA.COM. ¿Qué Es Hardening? {En línea} {30 de septiembre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/).

de información, sean atacados. Esta herramienta es capaz de prevenir los ataques antes de que se realicen. La importancia de este tipo de tecnología radica, en que a diario surgen miles y miles de formas para atacar todo tipo de sistemas de información, que pueden proceder bien sea de fuentes internas o externas.

CARACTERISTICAS DE UN SISTEMA SIEM

- "Recolectar información de diferentes dispositivos.
- Normalizar la información recolectada, organizándola por fecha y hora, para que sea más fácil realizar las búsquedas en posibles listas u otro tipo de archivos a la hora de necesitarla.
- Analizar la información.
- Tener un módulo de gestión para que a través de este se puedan administrar las soluciones que se generen por amenazas".[10]

HERRAMIENTAS PARA LA CONTENCION DE ATAQUES

- FIREWALL HARDWARE
- FIREWALL SOFTWARE
- ANTIVIRUS

FIREWALL HARDWARE: dispositivo físico electrónico externo de red y autónomo que conecta diferentes redes gracias a una interfaz de red integrada. Este cortafuego revisa todos los datos que ingresan de internet, dejando pasar los paquetes de datos que son seguros y bloquea automáticamente los paquetes de

[10] SOFECOM. SIEM, La Tecnología Capaz de Detectar y Neutralizar las Amenazas Informáticas Antes de que Ocurran. {En línea} {30 de septiembre de 2020} disponible en: (https://sofecom.com/que-es-un-siem/).

datos que representan peligro, garantizando con ello la seguridad de la red. Este tipo de cortafuego siempre está activado, requieren de una configuración experta, se usan principalmente para proteger de manera segura y robusta a las redes locales de empresas, para muchos son dispositivos complejos y la administración de los mismos suele ser también compleja de realizar.

FIREWALL SOFTWARE: "es una aplicación que se puede instalar en una computadora, también se les conoce como desktop firewall o software firewall, son aplicaciones básicas que generalmente se instalan en pequeñas instalaciones como un equipo de cómputo en un hogar o en un lugar de trabajo muy pequeño. La función de este cortafuego es la monitorear todos los puertos abiertos en un servidor web y verifica la información de cada puerto. El firewall tiene una lista de aplicaciones para ingresar a internet en ciertos puertos por lo tanto si la aplicación está utilizando un puerto específico, el software verifica el contenido de los datos que están ingresando y si son seguros los dejara pasar hacia la computadora, pero si una aplicación no verificada intenta ingresar a la información el sistema bloqueara la información entrante y saliente y realizara una notificación al usuario que el programa está intentando acceder a internet".[11]

Los firewall gratuitos se incluyen con el sistema operativo y normalmente son de uso personal, son fáciles de instalar, ya vienen activados, es la herramientas más básica debe tener todo PC para garantizar condiciones de seguridad básicas.

Se puede tener ambos firewall instalados e activados, puesto que el hardware protege al sistema del mundo exterior y el software protege al sistema de manera interna de otros sistemas que resulten ser dañinos para el mismo.

Entre los mejores Firewall gratuitos para sistemas Windows se encuentran:

---

[11] TECNOLOGIA INFORMATICA. Que es un Firewall y como funciona. Tipos de firewall. {En línea} {01 de octubre de 2020} disponible en: (https:/www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/)

- TinyWall
- Netdefender
- Glasswire
- PeerBlock

ANTIVIRUS: “son aplicaciones diseñadas para prevenir, bloquear, detectar y eliminar archivos dañinos que se descargan en el computador cuando se navega por internet y que están diseñados para atacar, dañar y modificar un sistema informático, comprometiendo la seguridad del mismo. Su función es la de proteger el sistema de los virus que existen y eliminar este tipo de amenazas”.[12]

La instalación de un buen antivirus junto con los firewall permite una mejor protección a un sistema informático y garantizan la seguridad del mismo.

Entre los antivirus reconocidos están:

- Bitdefender
- Norton
- Panda
- McAfee
- BullGuard

PRACTICA PARA EVITAR VULNERABILIDADES DEL SISTEMA (MAQUINA VIRTUAL WINDOWS 7 64 bits)

Para evitar vulnerabilidades en el sistema se desarrollan las siguientes acciones:

[12]CONCEPTO.D. Antivirus Informatico. {En línea} {01 de octubre de 2020} disponible en: (https://www.concepto.de/antivirus-informatico/).

Activar Cortafuegos.

Activar Windows Defender.

Activar Actualizaciones Automaticas.

Figura No. 10 Recomendaciones de seguridad que arroja el sistema:

Fuente: Autor

Instalar los correspondientes parches de seguridad, aunque el soporte técnico de win 7 finalizo el 14 de enero de 2020, de todas maneras se lleva a cabo el proceso de instalar todas las actualizaciones del sistema operativo, garantizando con ello la seguridad del sistema y minimizando los riesgos de vulnerabilidad del mismo.

VIDEO

https://youtu.be/uqaRuz_MRvI

CONCLUSIONES

Al finalizar el desarrollo del presente informe se concluye que:

La seguridad de un sistema informático es tema de vital importancia dentro de cualquier organización, ya que garantiza la protección de los datos o información manejados dentro de la misma.

En toda organización es necesario que se constituya o exista el área de seguridad informática, conformada por el personal idóneo, para llevar a cabo todas las tareas que impliquen única y exclusivamente, el manejo de la seguridad del sistema informático.

El equipo o personal encargado del área de seguridad, en todo momento deberá tener plenos conocimientos, de todos los temas en cuanto a seguridad informática se requieren, para el adecuado manejo y administración de la seguridad del sistema.

El equipo o personal encargado de la seguridad del sistema, deberá tener las habilidades necesarias para proponer y ejecutar estrategias, que permitan neutralizar los ataques informáticos, utilizando para ello todas las herramientas y acciones adecuadas que permitan frenar los mismos.

Al hacer parte de un equipo de trabajo para la seguridad de un sistema, o parte del personal responsable de la seguridad del sistema, se requiere que se tenga conocimiento sobre las normas que se tipifican como delitos informáticos, con el fin de no incurrir en ese tipo de conductas, garantizando con ello la seguridad de la información y la integridad de quienes están relacionados estrechamente, con el sistema informático.

RECOMENDACIONES

Con el fin de mejorar la seguridad de los sistemas informáticos dentro de cualquier tipo de organización se recomienda:

La creación de un equipo de trabajo, con personal capacitado para el manejo exclusivo de la seguridad del sistema, en caso de que la organización no maneje este tipo de recursos.

Las capacitaciones cada cierto tiempo, con el fin de que las personas encargadas del manejo de la seguridad del sistema, estén actualizadas con todos los temas, que tienen que ver con seguridad informática.

Establecer un manual para el desarrollo de buenas prácticas de seguridad, en las que apliquen todas las acciones y herramientas necesarias para garantizar la seguridad del sistema.

La ejecución de auditorías para el equipo o área encargada de la seguridad del sistema, con el fin analizar cada una de las labores realizadas para mantener la seguridad del mismo y que permitan determinar si cumplen con los objetivos propuestos para tal fin.

La ejecución de auditorías para todos los usuarios del sistema, con el fin de hacer un seguimiento detallado del manejo y de las acciones que realizan sobre el sistema, para evitar posibles fugas de información a través de los usuarios.

Se proponen capacitaciones para todos los usuarios del sistema, con el fin de educarlos en la importancia de la seguridad informática y en el manejo de herramientas sencillas que pueden manejar para contribuir al mejoramiento de la seguridad del sistema.

Se propone al equipo de seguridad, llevar a cabo prácticas o procesos, que permitan la intrusión o penetración al sistema, con el fin de evaluar las vulnerabilidades del mismo y de esa forma aplicar soluciones que erradiquen estas vulnerabilidades.

BIBLIOGRAFIA

THREATPOST. Overlay Malware Target Windows Users with a DLL Hijack Twist. {En línea} {30 de septiembre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/).

GRAHAMCLULEY. Grindr Security Hole Made it Easy to hijack Accounts. {En línea} {01 de octubre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/)

DARKREAING. A 7 Step Cybersecurity Plan For Healtcare Organizations. {En línea} {01 de octubre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/)

SCHENEIER. Hacking Apple For Profit . A 7 Step Cybersecurity {En línea} {01 de octubre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/)

WIRED. US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit. {En línea} {02 de octubre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/)

HACKERUNA.COM. ¿Qué Es Hardening? {En línea} {30 de septiembre de 2020} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/).

GUILLÉN ZAFRA, José Luis. "Introducción al pentesting". Barcelona, 2017. 66p. {En línea} {30 de septiembre de 2020} disponible en (http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf)

SOFECOM. SIEM, La Tecnología Capaz de Detectar y Neutralizar las Amenazas Informáticas Antes de que Ocurran. {En línea} {30 de septiembre de 2020} disponible en: (https://sofecom.com/que-es-un-siem/).

NSIT. ¿Qué es SIEM en Seguridad Informática? Alcance e Implementación {En línea} {30 de septiembre de 2020} disponible en: (https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/).

LEY 1273 DE 2009. Formato PDF. {En línea} {08 de septiembre de 2020} disponible en:

(https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

REVITA SEGURIDAD. CATORIA, Fernando. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. {En línea} {08 de septiembre de 2020}. Disponible en: (https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra)

BYTE MIND. Escaneando la Red con Nmap en Kali Linux. {En línea} {09 de septiembre de 2020} disponible en: https://byte-mind.net/escaneando-la-red-con-nmap/).

CONSEJO PROFESIONAL NACIONAL DE INGENIERA COPNIA. República de Colombia. Código de ética para el ejercicio de la Ingeniera en general y sus profesiones afines y auxiliares. {En línea} {07 de septiembre de 2020} disponible en: (https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica).

ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. {En línea} {09 de septiembre de 2020} disponible en: (https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/).

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA, Anexo 3, Acuerdo.

TECNOLOGIA INFORMATICA. Que es un Firewall y como funciona. Tipos de firewall. {En línea} {01 de octubre de 2020} disponible en: (https:/www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/)

CONCEPTO.D. Antivirus Informático. {En línea} {01 de octubre de 2020} disponible en: (https://www.concepto.de/antivirus-informatico/).