UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2019–MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

Análisis para Detectar Amenazas y Vulnerabilidades en la Red del ITSB de la ciudad de Babahoyo

EGRESADA:

Andrea Estefanía Lucio Troya

TUTORA:

Ing. Nelly Karina Esparza Cruz

AÑO 2020

RESUMEN

Los avances tecnológicos se están presentando en nuestro medio de forma muy común, es por eso que la mayoría de las organizaciones están implementado la informática en sus instalaciones con el objetivo de por automatizar procesos para mejorar la calidad de sus servicios. Pero debido a esto nace la necesidad de mantener la seguridad de la información que se gestiona en la red, para que esta no sea vulnerada, robada o plagiada. En la actualidad el ITSB, presenta varios problemas con la red y la infraestructura, al no tener implementada una correcta política de seguridad, existen conflictos con direcciones IP, fallas en los equipos informáticos, infecciones de virus y poco mantenimiento preventivo a la infraestructura de Red. La metodología que se va a emplear es la descriptiva ya que permite conocer las situaciones predominantes a través de la descripción exacta de las actividades y procesos que realiza la red informática en el ITSB. El presente caso de estudio está conformado por tres fases las cuales son: identificación de activos, detección de vulnerabilidades y análisis de vulnerabilidades. Los resultados obtenidos en el presente estudio demuestran que existen vulnerabilidades tanto de tipo físicas, como lógicas dentro de la red del ITSB, donde las de tipo lógico no tienen mayor relevancia si se aplican las configuraciones a tiempo. En cuanto a las físicas se deben tomar medidas necesarias porque representan un riesgo potencial que puede afectar a la integridad lógica como física de la infraestructura e información de la institución.

Palabras claves

análisis, detectar, vulnerabilidades, red, seguridad, informática

ABSTRACT

Technological advances are being presented in our environment in a very common way, which is why most organizations are implementing information technology in their facilities with the aim of automating processes to improve the quality of their services. But due to this the need arises to maintain the security of the information that is managed in the network, so that it is not violated, stolen or plagiarized. At present, the ITSB presents several problems with the network and infrastructure, since it has not implemented a correct security policy, there are conflicts with IP addresses, computer equipment failures, virus infections and little preventive maintenance of the Network infrastructure The methodology that is going to be used is the descriptive one since it allows to know the predominant situations through the exact description of the activities and processes carried out by the computer network in the ITSB. The present case study consists of three phases which are: asset identification, vulnerability detection and vulnerability analysis. The results obtained in the present study demonstrate that there are vulnerabilities of both physical and logical types within the ITSB network, where those of logical type are not more relevant if the configurations are applied in time. As for the physical ones, necessary measures must be taken because they represent a potential risk that can affect the logical and physical integrity of the institution's infrastructure and information.

Keywords

analysis, detect, vulnerabilities, network, security, computing

INTRODUCCIÓN

Los avances tecnológicos se están presentando en nuestro medio de forma muy común, es por eso que la mayoría de las organizaciones están implementado la informática en sus instalaciones con el objetivo de por automatizar procesos para mejorar la calidad de sus servicios. Pero por el hecho de automatizar las diferentes tareas que se realizan de manera manual, nace otra necesidad para la organización que es mantener la seguridad de la información que se gestiona en la RED, para que esta no sea vulnerada, robada o plagiada.

El Instituto Tecnológico Superior Babahoyo (ITSB), actualmente presta las instalaciones de la Unidad Educativa Babahoyo, para ofertar carreras de tercer nivel. Está ubicado en la ciudad de Babahoyo en la avenida Enrique Ponce Luque, frente al terminal terrestre de la ciudad. La red del ITSB no se encuentra correctamente estructurada, por lo consiguiente se realizará un análisis para detectar vulnerabilidades en dicha red, porque si no se toman las medidas necesarias esto puede provocar riesgos que atenten a la seguridad de la información. El presente caso de estudio tiene como objetivo detectar amenazas y vulnerabilidades que pueden existir tanto en la infraestructura física como lógica de la red del ITSB, mediante un escaneo de la red utilizando la herramienta de escaneo Nessus.

En la actualidad el ITSB, presenta varios problemas con la red y la infraestructura, al no tener implementada una correcta política de seguridad, existen conflictos con direcciones IP, fallas en los equipos informáticos, infecciones de virus y poco mantenimiento preventivo a la infraestructura de Red. Existen: criterios que al cumplirse correctamente garantizan un perfecto funcionamiento de la red, los cuales velan por la seguridad y la integridad de la información. Tener políticas perfectamente establecidas garantiza la seguridad de los datos por los cuales se transmiten entre los diferentes puntos de la misma.

Los resultados del presente análisis ayudan a tener un visión clara de las amenazas físicas o lógicas que pueden existir la red de datos del ITSB; y con estos resultados el administrador de la red puede corregir las fallas que puedan existir aplicando las políticas de seguridad adecuadas para que no existan fugas de información; garantizando así que se cumplan los tres objetivos principales de la seguridad informática los cuales son la confidencialidad, integridad y disponibilidad de la información.

La metodología que se va a emplear es la descriptiva ya que permite conocer las situaciones predominantes a través de la descripción exacta de las actividades y procesos que realiza la red informática en el ITSB, los datos se expresaran en términos cualitativos ya que proporcionan una gran cantidad de información valiosa. El presente estudio, tiene relación a la línea de investigación de desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos basándose el análisis en la sublínea de investigación de procesos de transmisión de datos y telecomunicaciones.

Cabe recalcar, que en el presente caso de estudio sólo se realizará un análisis en la red para luego proponer las recomendaciones necesarias para minimizar los riesgos que pueden provocar el mal uso y la poca seguridad que tiene la red de la institución; mas no se realizarán cambios en la infraestructura o en la configuración de la red porque el presente proyecto tiene como objetivo informar del estado físico y lógico de la red.

DESARROLLO

La administración de seguridad se lleva a cabo en un panorama en constante cambio de nuevos sistemas, nuevas vulnerabilidades y nuevas herramientas. A medida que evolucionan las amenazas a la seguridad informática, también lo hacen las prácticas y herramientas de la administración de seguridad. En un nivel, las computadoras se están utilizando en grandes cantidades y en aplicaciones más amplias, lo que obliga a los administradores de seguridad a lidiar con volúmenes cada vez más grandes de información y, en consecuencia, a exigir más herramientas a sus herramientas. (Yaque, 2017)

A veces, las infracciones de seguridad aprovechan las múltiples vulnerabilidades en los sistemas, lo que hace que los patrones de ataque sean difíciles de predecir. Como resultado, los administradores de seguridad necesitan saber cómo funcionan e interactúan los distintos dispositivos y sistemas para analizar las situaciones en desarrollo. Si bien la mayoría de los ataques de virus parecen tener el objetivo de interrumpir las operaciones de la computadora, la mayoría de los ataques dirigidos por humanos apuntan a obtener el control de las máquinas. Estos privilegios se utilizan para atacar otras máquinas, robar datos o recursos computacionales, y ocasionalmente destruir datos.

En la actualidad, un tema de suma importancia es la seguridad informática debido a que existen agentes que pueden dañar la integridad de los datos que se manejen en una organización. La seguridad informática abarca el resguardo tanto de los equipos, infraestructura, redes informáticas, los usuarios que hacen uso de estas tecnologías y sobre todo la información que se produce a través de las operaciones diarias en la organización. Siendo esta última el activo más importe de una empresa, si se manipula incorrectamente, se cambia su integridad o cae en manos de personas no autorizadas puede provocar serios problemas y pérdidas económicas y/o materiales. (DORDOIGNE, 2015)

Es por eso que la seguridad de la información es de suma importancia en las organizaciones de hoy en día. La seguridad de la información, se refiere a los procesos y herramientas diseñados e implementados para proteger la información comercial confidencial de modificaciones, interrupciones, destrucción e inspección. La información puede ser física o eléctrica. La información puede ser similar a sus detalles o podemos decir su perfil en las redes sociales, sus datos en el teléfono móvil, sus datos biométricos, etc. Por lo tanto, la seguridad de la información abarca tantas áreas de investigación como criptografía, informática móvil, ciber forense, redes sociales en línea, etc. (CARPENTIER, 2016)

El Instituto Tecnológico Superior Babahoyo (ITSB), actualmente ejerce sus actividades académicas y administrativa en las instalaciones de la Unidad Educativa Babahoyo, ubicada en la Av. Enrique Ponce Luque, frente al terminal terrestre, es decir que el instituto realiza sus activados en instalaciones prestadas. El problema radica en que, al hacer uso de las instalaciones prestadas, este no puede invertir en una infraestructura tecnológica adecuada para la gestión de los procesos informáticos que se realizan a diario en la red de datos de esta institución de educación superior.

Si bien es cierto, en los últimos 20 años se ha ido implementado sistemáticamente el uso de las tecnologías de la información en las instituciones educativas. Los sistemas de información policial, que antes se basaban en el cotejo de fichas a cargo de un archivero, han evolucionado con el uso de las tecnologías de la información hasta convertirse en departamentos que utilizan programas informáticos especiales para garantizar la calidad educativa.

La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos,

como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información. (Baca, 2016)

Una amenaza informática está relacionada con la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y los sistemas de información. Las amenazas son consideradas como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización. (Chicano, 2019)

El presente estudio de caso se basa en la metodología la investigación descriptiva, porque se pretende analizar y describir el estado físico de la red informática que usa el instituto, usando como herramienta la entrevista, el cuestionario como instrumento y la observación como técnica, donde se desea obtener información más detallada acerca de la red del lugar. También se usa como herramienta tecnológica a Nessus, para realizar un escaneo lógico y detectar vulnerabilidades que pueden existir dentro la configuración de la red.

El presente caso de estudio está conformado por tres fases las cuales son: identificación de activos, detección de vulnerabilidades y análisis de vulnerabilidades. Para la identificación de activos se procedió a la visita al lugar y se realizó una entrevista al administrador de la red. Para la detección de vulnerabilidades físicas se utilizó una ficha de observación y para las vulnerabilidades lógicas se usó Nessus Escáner para detectar malas configuraciones en el sistema operativo de los terminales o en los equipos de red. Y por último se realiza un análisis de las vulnerabilidades y recomendar las soluciones pertinentes para evitar riesgos en un futuro.

Nessus es uno de los muchos escáneres de vulnerabilidades utilizados durante las evaluaciones de vulnerabilidad y las pruebas de penetración, incluidos los ataques maliciosos. Este artículo se centrará en este escáner de vulnerabilidades, discutiendo los fundamentos que uno necesita tener antes de comenzar con la herramienta, las diferentes capacidades de escaneo que proporciona, lo que se necesita para ejecutar la herramienta y cómo aparecen los resultados una vez que se completan los escaneos. (Jetty, 2018)

El presente caso de estudio no pretende realizar ningún tipo de cambios en las configuraciones en las topologías, enlaces o en los equipos, ni tampoco realizar la compra la compra de equipamientos adicionales como routers, switchs o modificaciones físicas en la infraestructura. Tampoco contempla cotizaciones especializadas de seguridad en redes LAN.

Una evaluación de vulnerabilidad es el proceso de identificar y clasificar cualquier agujero de seguridad en su red o sistemas de comunicación. Al analizar aspectos vitales de su gestión de datos, usted determina la efectividad de su software de seguridad actual y cualquier medida adicional que deba tomarse.

El enfoque clave de un análisis de vulnerabilidad es:

- Definir y clasificar los recursos de red y / o sistema.
- Identificar posibles amenazas a estos recursos.
- Desarrollar una estrategia para enfrentar las amenazas más graves.
- Definir e implementar formas de minimizar la probabilidad de que estas amenazas se vuelvan más graves y las consecuencias resultantes.

A medida que se crean nuevos virus y la tecnología cambia, debe asegurarse de que su software de seguridad esté preparado para manejar las últimas amenazas. Para una empresa interesada en proteger su seguridad y reputación comercial, los investigadores de

ciberseguridad recomiendan aprovechar todas las oportunidades disponibles para garantizar que la infraestructura de su red esté protegida adecuadamente para resistir la presión de los intrusos. Realizar evaluaciones de vulnerabilidad de la red y pruebas de penetración de manera regular, trimestralmente o al menos una vez al año, es un paso indispensable para prepararse para una variedad de desafíos de ciberseguridad.

Durante la fase 1 se procedió a la realizar la visita al instituto y se pudo observar el estado de la red informática de la institución. La red no tiene una configuración estructurada, los cables se desplazan de departamento a departamento sin la protección adecuada, no poseen regletas, lo que puede provocar el deterioro de los mismos. Por otro lado se cuenta con switch el cual distribuye la red hacia varios departamentos, este se encuentra a la vista de todos sin ninguna protección ni la existencia de un rack, y cualquier persona no autorizada lo puede manipular.

En la entrevista el administrador manifestó que la red informática se encuentra en ese estado porque la institución no se encuentra en instalaciones propias, por eso se invierte en mejorar la infraestructura tecnológica porque en cualquier momento ellos pueden salir de ahí, por ahora la red funciona y cumple con los objetivos que tiene la organización. Pero, aunque este argumento tenga sentido, resulta peligroso que una red esté expuesta de esa manera porque por ese medio se transmite información muy importante para la institución.

El cable estructurado permite realizar las conexiones de punto a punto, y asegura que la conexión sea fiable y funcional. Al diseñar una red, se debe tener en cuenta el factor de riesgo físico en el que puede encontrarse cada componente que la conforma, sujeto a robos, sabotajes u otros factores. Cuando comenzamos el proceso de implementación de una red, debemos tener el concepto de seguridad intrínseco en nosotros, ya que la red puede ser diseñada de una manera óptima según nuestro criterio, pero estar sujeta a mal funcionamiento

por interferencias magnéticas, robo de equipamiento y sabotajes o vandalismo. Por este motivo, la seguridad física es un aspecto clave en esta etapa. (Lederkremer, 2019)

Todos estos riesgos mencionados se pueden suscitar en el ITSB, debido a que no se han tomado las precauciones pertinentes para mantener la red. Esto puede provocar que existan interferencias porque los cables se encuentran sin protección, además de exista un deterioro de los mismos debido a que están expuestos al ambiente. Los riesgos más comunes para el cableado pueden resumirse en los siguientes:

- *Interferencias*: pueden ser generadas por cables de alimentación de maquinaria pesada que emitan radiaciones electromagnéticas, o por equipos de radio o microondas. Al tener contenido metálico, los cables se ven afectados.
- *Corte del cable*: la conexión establecida se rompe, IO que impide que el flujo de datos circule por el cable.
- *Daños generados en el cable*: los daños normales con el uso hacen que las comunicaciones dejen de ser fiables.

Esta institución cuenta con una red de datos la cual comparte conexiones con tres departamentos y con los laboratorios de informática. La topología de la red es en árbol, debido a que tienen creado diferentes puntos de conexión de los cuales salen los diferentes nodos de conexión. Tiene dos laboratorios en los cuales hay un total de 45 computadoras de escritorio y cuya conexión se realiza de forma inalámbrica.

La topología de un árbol es un tipo especial de estructura en la que muchos elementos conectados están dispuestos como las ramas de un árbol. Por ejemplo, las topologías de árbol se usan con frecuencia para organizar las computadoras en una red corporativa, o la información en una base de datos. En la figura 1 se muestra el esquema general de esta

topología. En una topología de árbol, solo puede haber una conexión entre dos nodos conectados. Debido a que dos nodos pueden tener solo una conexión mutua, las topologías de árbol crean una jerarquía natural primaria y secundaria. (Torres Llamas, 2015)

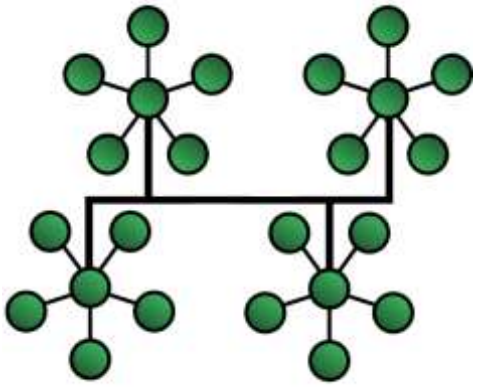


Fig. 1. Esquema General de la topología en árbol. Autor (Torres Llamas, 2015)

Durante la identificación de los activos se pudo constatar que los equipos tanto de red como los terminales se encuentran en buen estado, pero en general existe un desorden total en lo que la red se refiere. En los laboratorios no existe como tal ese tipo de desorden debido a que las computadoras se conectan inalámbricamente y por ende no existen la gran cantidad de cables que existe en los otros departamentos de la institución.

En la fase II, se procedió a realizar un escaneo interno de la red usando la herramienta Nessus Escáner. El propósito de este escaneo es identificar las vulnerabilidades existentes en la red. Todas las computadoras tienen como sistema operativo Windows 7, permitiendo así la compatibilidad para poder realizar el escaneo de forma exitosa. Nessus es una herramienta de escaneo de seguridad remota, que escanea una computadora y genera una alerta si descubre cualquier vulnerabilidad que los piratas informáticos maliciosos puedan usar para acceder a cualquier computadora que haya conectado a una red.

Cada computadora tiene miles de puertos, todos los cuales pueden o no tener servicios (es decir, un servidor para un protocolo específico de alto nivel) escuchándolos. Nessus funciona probando cada puerto en una computadora, determinando qué servicio está ejecutando, y luego probando este servicio para asegurarse de que no haya vulnerabilidades en él que pueda ser utilizado por un hacker para llevar a cabo un ataque malicioso. Nessus es llamado "escáner remoto" porque no necesita ser instalado en una computadora para que pueda probar esa computadora. En su lugar, puede instalarlo en una sola computadora y probar tantas computadoras como desee.

En la fase III, el resultado del escaneo de la red se analizó que la configuración de los equipos de red se encuentra correctamente aplicada, sin embargo los equipos de escritorio presentan fallas en su configuración. En este resultado el escaneo muestra, que existen tres tipos de vulnerabilidades alto, medio y bajo correspondientemente. La vulnerabilidad de tipo alto, hace énfasis a que el servicio de compartir impresoras en la red no tiene privilegio, lo que quiere decir que cualquier usuario ajeno a la institución que se conecte a red puede utilizar la impresora sin necesidad de autenticación.

La vulnerabilidad de estado medio representa que el mismo servicio de impresoras de red puede ser usado por un usuario que no tenga firma digital. La vulnerabilidad de estado bajo, dice que se pudo detectar la información que del servicio de DHCP. Es decir que cualquier usuario ajeno a la institución tendrá acceso a la red. Los otros 35 resultados son simple notificaciones que no tienen riesgo alguno en lo que a la seguridad se refiere, pero se deben tomar en cuenta ya que revelan información relevante de la red.

Los resultados obtenidos en el presente estudio demuestran que existen vulnerabilidades tanto de tipo físicas, como lógicas dentro de la red del ITSB, donde las de tipo lógico no tienen mayor relevancia, debido a que si se aplican las configuraciones pertinentes, estas

vulnerabilidades no representan mayor riesgo, en cuanto a las físicas se deben tomar medidas necesarias porque representan un riesgo potencial que puede afectar a la integridad lógica como física de la infraestructura e información de la institución.

La seguridad física a menudo se pasa por alto, y se subestima su importancia, en favor de amenazas más técnicas como piratería informática, malware y ciberespionaje. Sin embargo, las violaciones de la seguridad física pueden llevarse a cabo con fuerza bruta y poco o ningún conocimiento técnico por parte de un atacante. La seguridad física tiene tres componentes importantes: control de acceso, vigilancia y pruebas. Deben colocarse obstáculos en el camino de los atacantes potenciales y los sitios físicos deben endurecerse contra accidentes, ataques o desastres ambientales. (Romero, 2018)

El primer nivel de seguridad en cualquier red informática es la seguridad física. La seguridad física es importante para las estaciones de trabajo pero vital para los servidores. Cualquier hacker que valga la pena puede vencer rápidamente todas las medidas de seguridad menos paranoicas si puede obtener acceso físico a un servidor. Las computadoras cliente también deben ser físicamente seguras. Debe indicar a los usuarios que no dejen sus computadoras desatendidas mientras están conectados. En áreas de alto tráfico, los usuarios deben asegurar sus computadoras con la cerradura. Además, los usuarios deben cerrar las puertas de sus oficinas cuando salgan. (Daswani, 2018)

Por otra parte el cableado de la red debe tener su estructura adecuada para evitar inconvenientes. Una instalación de cableado deficiente puede causar zonas inactivas de WiFi de diferentes maneras. La ubicación de su enrutador cuando la red está configurada puede tener grandes repercusiones en su conectividad a Internet. Al trabajar con cables de cobre al aire libre, un se debe considerar de interferencia electromagnética cercana. La interferencia electromagnética puede ser inducida por la presencia de equipos eléctricos como motores,

aires acondicionados, luces fluorescentes y líneas eléctricas. Desafortunadamente, cuando hay ruido electromagnético, interfiere con la transmisión de señales.

Cuando se trabaja con una combinación de cableado de cobre y fibra, la colocación del cable se convierte en un factor importante en la calidad de su red. Si los cables de cobre se colocan con demasiado peso sobre los cables de fibra, entonces los cables de fibra podrían aplastarse y requerir la instalación de cables nuevos. Si no se está al tanto de los requisitos de radio de curvatura y peso para los cables de fibra, podrían usar bridas de cableado para unir los cables. Esto crea un mayor radio de curvatura y pérdida de señal que ralentiza su red. (Martín, 2019)

Un diseño de red eficiente implica cables de alta tecnología correctamente agrupados con una alta densidad de puertos. Una manera fácil de evaluar la eficiencia de su diseño es contar el número de puertos por unidad de espacio en rack. Cuanto mayor sea el recuento de puertos, mejor será la eficiencia de su diseño.

La eficiencia del diseño hace que sea más fácil trabajar con sus cables. Los cables deben estar debidamente etiquetados y organizados para que sean fáciles de trabajar y se vean bien. Una oficina con cableado esparcido por el piso y enredado dentro de la sala de servidores disminuye la eficiencia de su red y hace que sea más difícil trabajar con el cableado en caso de necesitar algún trabajo. Cuando trabaja con un buen contratista de cableado, su red de TI debe verse ordenada y ordenada con etiquetas fáciles de leer. (Rivera, 2016)

CONCLUSIONES

El presente caso de estudio, tuvo como finalidad establecer en qué estado se halla la seguridad de la red de datos del Instituto Superior Tecnológico Babahoyo, y según observaciones y aplicando la herramienta Nessus se determinó que existen pocas vulnerabilidades en la configuración lógica y que pueden ser corregidas oportunamente. Además se determinó que la infraestructura no está completa en su totalidad, a red necesita estructurarse y mejorar su infraestructura.

La seguridad informática es un tema muy importante que deben tomar en cuenta las instituciones antes de la instalación y durante el uso de infraestructura tecnologías. La información es el activo más valioso de una institución educativa, es por ello que aunque el ITSB no labore en instalaciones propias debería invertir un poco más para mejorar su infraestructura tecnológica de red, porque perder información por la mala administración e infraestructura de la red puede ocasionar consecuencias muy graves en un futuro,

El ITSB necesitaba un nuevo enfoque para su proceso de seguridad en su red. "La mayoría de las organizaciones como la estas se enfrentan a un aluvión de ataques todos los días. La mayoría de ellos no tienen éxito, pero el gran volumen puede ser una distracción que dificulta determinar si algo ha pasado. Por eso se debe utilizar herramientas adicionales, para ser capaz de identificar mejor las amenazas y responder en consecuencia.

En lo que respecta a la herramienta utilizada en el presente caso de estudio, aunque en el ITSB presenta pocas vulnerabilidades en su configuración lógica, se pudo concluir Nessus es una de las mejores herramientas para la detención y reparación de vulnerabilidades existentes en una Red, en comparación con otras herramientas. Nessus posee más complementos

destinados para el análisis de tráfico de red y sobre todo su facilidad de instalación y usabilidad.

BIBLIOGRAFÍA

Baca, G. (2016). *Introducción a la seguridad informática.* Grupo Editorial Patria.

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: Ediciones ENI.

Chicano, E. (2019). *Auditoría de seguridad informática. IFCT0109.* IC Editorial.

Daswani, D. (2018). *La amenaza hacker.* Grupo Planeta.

DORDOIGNE, J. (2015). *Redes informáticas - Nociones fundamentales.* Ediciones ENI.

Jetty, S. (2018). *Network Scanning Cookbook: Practical network security using Nmap and Nessus 7.* Packt Publishing Ltd.

Lederkremer, M. (2019). *Redes Informáticas.* Buenos Aires: RedUsers.

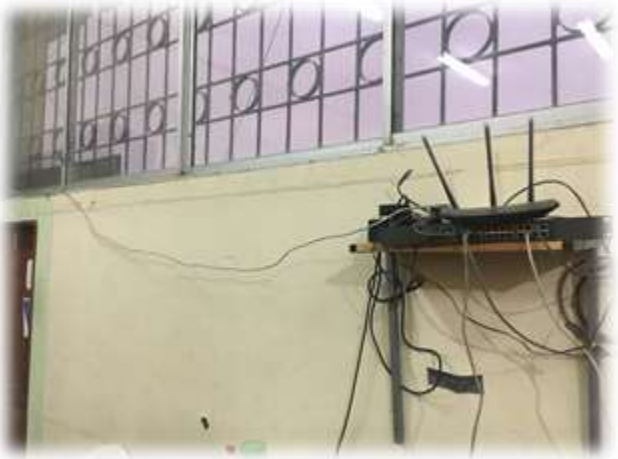
Martín, J. (2019). *Redes de datos y su cableado (FPB Instalaciones de telecomunicaciones).* Editex.

Rivera, J. (2016). *Fundamentos de Redes Informáticas: 2ª Edición.* IT Campus Academy.

Romero, M. (2018). *NTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* 3Ciencias.

Torres Llamas, R. (2015). *UF0854 - Instalación y configuración de los nodos de una red de área local.* Madrid: Editorial Elearning, S.L.

Yaque, A. (2017). *Seguridad en el montaje y mantenimiento de redes y distribución de agua y saneamiento. ENAT0108.* IC Editorial.




TP-LINK


TP-LINK
NOTOCAR

FICHA DE OBSERVACIÓN

<table>
<tr><td rowspan="2">Ficha de Observación</td><td>Caso de Estudio: Análisis para Detectar Amenazas y Vulnerabilidades en la Red del ITSB de la ciudad de Babahoyo</td></tr>
<tr><td>Responsable: Andrea Lucio</td></tr>
<tr><td>Fecha: 13 de enero de 2020

Hora: 16:30

Lugar: Instituto Tecnológico Superior Babahoyo.</td><td>OBSERVACIÓN
El ITSB ejerce sus actividades académicas y administrativas en las instalaciones de la unidad educativa Babahoyo, frente al terminal terrestre.
Se observó una red LAN y cableado, 1 switch, 1 router, 45 máquinas presentes en el laboratorio.
El cable es UTP categoría 6. Se usa una topología en Árbol, debido conectados desde al switch a los terminales, ya la salida al internet es por medio del router. Se notó que algunos cables se están deteriorando.
El cableado se encuentra disperso según como lo amerite el departamento, no cuenta con la seguridad y resguardo necesario.
El internet es obtiene con fibra óptica y por ende se utilizan conversores bridge, para que la conexión pueda ser usada normalmente por los equipos de red Ethernet</td></tr>
</table>

Resultados del análisis de la red con Nessus.

10.10.0.2

0	1	1	1	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 38

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	5.0	57608	SMB Signing not required
LOW	3.3	10663	DHCP Server Detection
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	25342	XMPP Server Detection