UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

Estudio de Amenazas y Vulnerabilidades en la Red de Comunicación del Departamento de Sistemas de la Universidad Técnica de Babahoyo

EGRESADO:

Yordy Alejandro Chonana Sosa

TUTOR:

Ing. María Isabel Gonzales Valero

AÑO 2018

TEMA: ESTUDIO DE AMENAZAS Y VULNERABILIDADES EN LA RED DE COMUNICACIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO.

I. INTRODUCCIÓN

Los sistemas computacionales hoy en día se han convertido en elementos importantes en el desarrollo de la sociedad, de un país y del mundo, estableciendo cambios en la manera cotidiana de vivir de los seres humanos, así como también de las empresas y organizaciones, que día a día se esfuerzan por mejorar sus servicios y llegar a lugares en donde no se podía llegar.

Pero para mantener estos sistemas surgen muchos mecanismos importantes los cuales nos permiten tener aquellos sistemas en un estado óptimo, de tal manera que puedan funcionar correctamente, reduciendo el índice de filtrado de información, así como de atacantes cibernéticos.

En la Universidad Técnica de Babahoyo se suscitó hace un tiempo atrás (2 años) un inconveniente con la red de datos, en los cuales se vio afectada la página principal de la universidad, debido a vulnerabilidades que existían en ese momento; por tal motivo es de suma importancia detectar los problemas a tiempo para así tomar las medidas adecuadas, para poder solucionar o mitigar dichos problemas, y de esta manera brindar un mejor servicio tanto a estudiantes como personal administrativo de la UTB.

En el presente trabajo se realizó un escaneo mediante dos herramientas muy conocidas en cuanto a seguridad, las cuales son Nessus y Nmap de Kali Linux, para de esta manera determinar las vulnerabilidades de la red de comunicación, así como también se hicieron las respectivas observaciones en cuanto al resultado de dicho análisis. Además, este trabajo está comprendido dentro de las líneas de investigación de la Universidad Técnica de Babahoyo, específicamente en la línea de Desarrollo de Sistemas de la Información, Comunicación y

emprendimientos empresariales y Tecnológicos, sublínea Proceso de Transmisión de Datos y Telecomunicaciones.

II. DESARROLLO

Con el avance de la tecnología y el constante crecimiento y desarrollo de esta, hacen que las herramientas tecnológicas se vuelvan muy indispensables y necesarias para el desarrollo de cualquier actividad, ya sea en la salud, en la innovación, en la educación, trasporte, etc.

Hoy en día las empresas e instituciones adoptan tecnología para estar a la par de las tendencias en comunicaciones, transmisión de datos, etc. además de estar enlazados desde cualquier parte del mundo y de esta manera tener acceso a su información; Hoy en día existen muchos servicios y equipos que brindan la capacidad de almacenar grandes volúmenes de información y albergar un sin números de páginas o sitios web, que es lo que comúnmente observamos en la red de internet en la cual muchas organizaciones se dan a conocer, tanto como organización así como también los productos o servicios que ofrecen.

Además de eso cabe mencionar que cada una de estas organizaciones o instituciones cuenta con una red interna, la cual la utilizan para compartir información y datos de suma importancia para ellas, la cual se debe administrar con mucho recelo debido a la importancia de la información que por ella se transmite, la cual no puede ser accesada por terceras personas ajenas a la organización. Por tal motivo es necesario establecer políticas de seguridad que ofrezcan un mejor desempeño en la red de datos de una organización, ya que esto ayudará a resguardar la integridad de la misma para evitar que personas maliciosas logren introducirse en la red, asegurando que los procesos que se realizan son confiables, así como el resguardo de los datos que se manejan en dicha red, la cual debe tener un departamento propio donde se albergue

los equipos que permiten la transmisión de dichos datos. Ya que existe el riesgo de que la información que se procesa en dicho departamento pueda filtrarse.

Como sabemos la información es el elemento más importante en cualquier organización ya que ella revela el estado actual y la evolución que ha venido experimentado la institución a través de los años. (Baca, 2016, p. 8) afirma que, "La información es entonces el activo más valioso de cualquier empresa, después del activo humano", permite la toma de decisiones, puede cambiar el rumbo de una organización, pero también puede ser perjudicial si es plagiada.

> Por otra parte, se requiere que una organización haga algo más que solo colocar defensas digitales; un porcentaje considerable de los ataques con éxito se originan en el mundo físico análogo o reciben ayudan y se agravan por vulnerabilidades físicas y ambientales. Una seguridad eficaz requiere por tanto un Sistema de Gestión de la Seguridad de la Información fuerte, sistemática e integral; los consejos, los clientes y los reguladores todos buscan una garantía de que se han identificado los riesgos de la información y están siendo gestionados. (calder, 2017, p. 9)

La metodología empleada en este estudio es el método inductivo, el cual permitió realizar un análisis general de la situación del departamento de sistemas y así poder llegar a una conclusión especifica esto a través de la observación, por otra parte para la recolección de información se realizó una investigación de campo la cual permitió conocer de qué manera está estructurado dicho departamento a través de una entrevista, misma que se llevó a efecto en dicho departamento con el Analista de Redes de la universidad Técnica de Babahoyo, quien facilito la recolección de información importante para el desarrollo de este estudio.

En la entrevista realizada al Analista del departamento de Sistemas Ing. Holger Paredes Zapata manifiesta que, el departamento de sistemas es el encargado de brindar seguimiento y soporte a toda la Universidad Técnica de Babahoyo, es decir a todas las facultades que la conforman. Además, está encargado de diseñar y crear sistemas dependiendo a las necesidades de la universidad, esto debido al grupo de Desarrolladores con los que cuenta.

Además, realizan monitoreos para administrar el ancho de banda que se suministra para cada facultad o departamento, así como también para evidenciar que el servicio de internet sea fluido y que no haya problemas de conectividad.

En él se encuentra el Data Center, en el cual se encuentran las conexiones de fibra óptica de los proveedores de internet, los servidores en cuya estructura se encuentran alojados cada uno de los sistemas que tiene la UTB.

Dicho departamento está conformado por:

- El administrador
- Analistas de redes
- Técnicos,
- Y laboratoristas en las distintas facultades que conforman la universidad técnica de Babahoyo.

En donde los laboratoristas, son los encargados solucionar los problemas que se puedan presentar en la facultad donde estén designados, en caso de que los problemas sean más complicados y que no puedan ser resueltos por ellos, entonces se comunica al departamento de sistemas, los cuales atenderán el caso y actuarán conforme sea necesario.

El departamento cuenta con equipos como Switch, servidores, Router, de marcas reconocidas como Dlink, Tplink, Microtick, Cisco, etc. Además, ha implementado un firewall

para filtrar el acceso a internet conocido como UTM Sophos el cual brinda una serie de herramientas para controlar el tráfico en la red de una manera rápida y eficiente; cuenta con sistemas IPS (Sistema de Prevención de Intruso) y IDS (Sistema de detección de Intruso), para evitar ataques de Spoofing, Fishing, etc. (Ireo, s.f)

DISPOSITIVOS	CRACTERISTICAS
Switchs	✓ Cisco, Dlink, y TpLink de 8, 24 y 48 canales ✓ 10/100Mbps ✓ Control de flujo
Routers	✓ Qpcom, TpLink, Dlink, de 2 antenas
Enlace de Radio	✓ Antena Ubiquiti Rocket Dish, ✓ Alcance**:** hasta 25km de distancia ✓ Velocidad de transmisión: hasta 150Mbps
UTM - Sophos	✓ Firewall con IDS, IPS, filtrado de red

Tabla 1. *Características de los dispositivos de red del departamento de Sistemas de la Universidad Técnica de Babahoyo.*
Desarrollado por: *Yordy Chonana Sosa*

La Universidad Técnica de Babahoyo experimentó un tipo de ataque a finales del año 2015 (entre diciembre del 2015 y enero del 2016), en la que terceros irrumpieron en la red de datos de la universidad y atacaron a la página principal, haciendo uso del ataque conocido como "Desfiguración de páginas web", a través del puerto 80, causando graves molestias ya que al cargar la página se redireccionaba a una página pornográfica, lo cual daba mal aspecto a la institución.

El Ing. Holger Paredes Zapata, manifestó que esto ocurrió debido a que no contaban con la licencia del protocolo Https en la página principal, lo que facilitó el acceso de los atacantes. Por otra parte, el Ing. Alexander Izquierdo, Programador del Dept. Sist. de la UTB, acotó que una causa más de este incidente fué la falta de actualización del CMS Joomla, el cual es un gestor de contenidos que permite crear de manera sencilla una página web (García, 2015).

La presente investigación tiene como objetivo realizar un estudio en el departamento de sistemas de la Universidad Técnica de Babahoyo (UTB), para constatar que vulnerabilidades pueden existir en dicho departamento, así como también a que amenazas puede estar expuesta la red de datos, realizando un análisis basado en la herramienta Nmap, incluida en el sistema operativo Kali Linux, el cual es una distribución de Linux.

Kali Linux está orientado a brindar seguridad a una red, en él se encuentran una serie de herramientas que pondrán a prueba nuestra red o sistema (Andres, 2016).

De igual manera se realizó el escaneo con un programa creado para esta misma tarea, detectar vulnerabilidades conocida como Nessus. "Nessus es una herramienta de análisis de vulnerabilidades de seguridad cuya funcionalidad es la de ayudar a detectar posibles vulnerabilidades en las maquinas escaneadas" (Castro, M., Díaz G., Alzórriz I.y Sancristóbal E, 2014, p. 292).

A través de esta herramienta se busca encontrar posibles "Huecos", los cuales puedan ser aprovechados por terceros para introducirse en la red, y de esta manera poder proteger dicha red contra ataques que comúnmente se hacen a las organizaciones, aprovechando ciertas vulnerabilidades de la red de datos para así causar daños, molestias, y en ocasiones el plagio de información.

Red de comunicación

Según (Gallego, 2015). "Podemos considerar una red de comunicación a aquella compuesta por dos o más entidades cuya finalidad es intercambiar información. Esta información, cuando se trata de equipos informáticos, viaja en forma de paquetes de datos, que contienen secuencias de ceros y unos (p. 8)".

Dichas redes de comunicación permiten la interconexión interna de toda una organización en este caso de la UTB, de tal manera que cada departamento existente puede comunicarse y compartir datos e información concerniente a la institución, así como comunicados que vienen desde el rectorado, el cual es el cargo más alto en la jerarquía de la institución.

¿Qué es vulnerabilidad?

> Se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como "agujeros de seguridad", pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc. (Escrivá, Romero, Ramada y Onrubia, 2013, p. 8)

De modo que las vulnerabilidades pueden presentarse incluso al no contar con personal especializado en la implementación de una red, ya que al realizar una mala configuración de la red estaría dejando un espacio a posibles ataques que la podrían comprometer seriamente, así como también la no utilización de firewall que controlen la comunicación o el tráfico de la red hacia el exterior, antivirus, etc.

¿Que son amenazas?

(Chicano. E, 2015), establece que, "Una amenaza es un conjunto de hechos y eventos que pueden ocurrir y provocar efectos perjudiciales a los activos del sistema de información".

Las amenazas se las considera como cualquier tipo de circunstancia que pueda atentar con el funcionamiento normal de la red de datos. Las amenazas se pueden dividir en dos partes

Amenazas pasivas. – son aquellas en las que el atacante busca interceptar la información que se transmite en la red sin modificarla, se estaría hablando de un tipo de espionaje de información y que pudiese ser revelada, un ejemplo de esto es el sniffing (Tropicode, 2017).

Amenazas activas. - (Escrivá et al., 2013) afirman que "son aquellas que realizan algún cambio que no ha sido autorizado en el estado del sistema, y estos son más peligrosos en comparación con las amenazas pasivas, ejemplo de esto tenemos la inserción de mensajes spam o el plagio de identidad".

La UTB como institución de educación superior maneja información de cada uno de los estudiantes que se han titulado y que ahora son profesionales, de tal manera que, si se llegase al filtrar dicha información, podría perjudicar a dichos profesionales, y no solo eso, sino que también existen gestiones que realizan internamente las autoridades de la UTB.

Es importante de igual manera realizar auditorías programadas ya que de esta manera se podrán evitar o detectar anomalías en la red de comunicación, y mantener la integridad de los datos que se transmiten en ésta.

Según (Administracion, s.f., párr. 1), afirma, "que la misma trata de realizar la verificación de los controles durante el procesamiento de la información, el desarrollo de los

sistemas y su instalación, con el fin de evaluar la efectividad que posee y presentar algunas sugerencias (siempre y cuando sea necesario) a la gerencia de la empresa".

De esta forma se puede conocer de manera más exacta el funcionamiento de los sistemas auditados, y así identificar la raíz de los posibles problemas encontrados; La auditoría permite a través de los resultados obtenidos, ejecutar planes de acciones y toma de decisiones a los administrativos de estos equipos, logrando así la eficiencia que se busca tener en el servicio que se presta. La auditoría de sistemas lógicamente se encarga de realizar un proceso de recolección y evaluación de evidencia para poder determinar los errores y características de un sistema.

Para realizar el análisis de la red de comunicación de la Universidad Técnica de Babahoyo se procedió de la siguiente manera:

Primeramente, se realizó un testeo para verificar que direcciones IP tenían cada máquina conectada al segmento de red 19, y cuál de ellas estaban activas, lo que resulto un total 254 máquinas activas con sus respectivas IP, tal como se muestra en la **figura 1.**

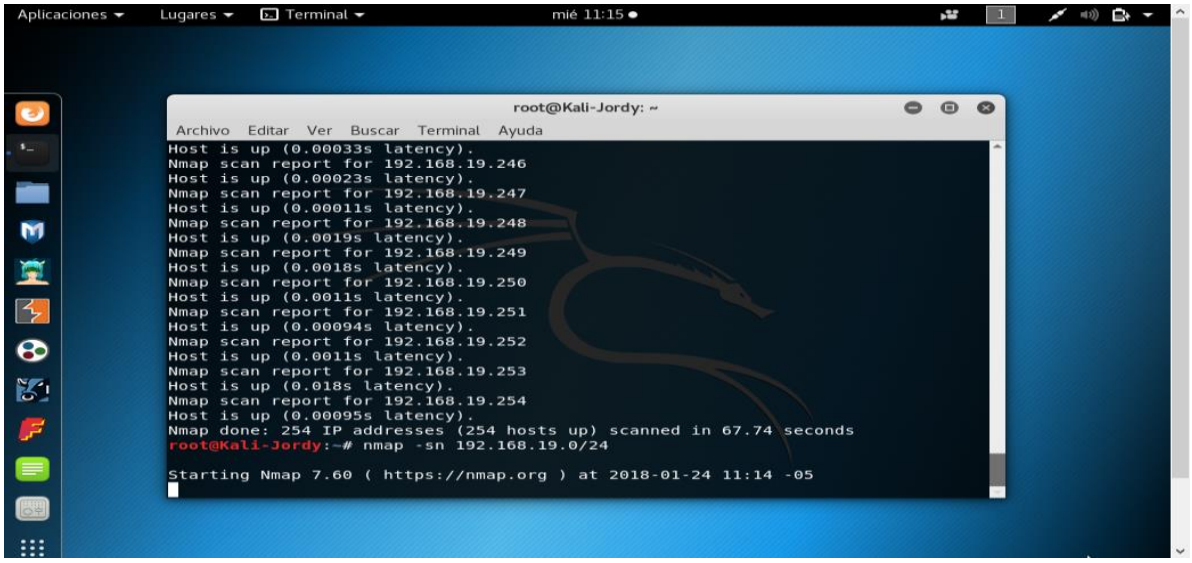

Figura 1. *Escaneo para verificar los equipos conectados en la red de comunicación de la Universidad Técnica de Babahoyo.*
Elaborado por: *Yordy Chonana Sosa*

Luego se procedió a realizar la comprobación de puertos abiertos y tome la IP de una maquina al azar de las que arrojo el primer análisis para ello se hizo uso del comando **nmap –sS –v 192.169.19.100. (Véase** en la **figura 2)**

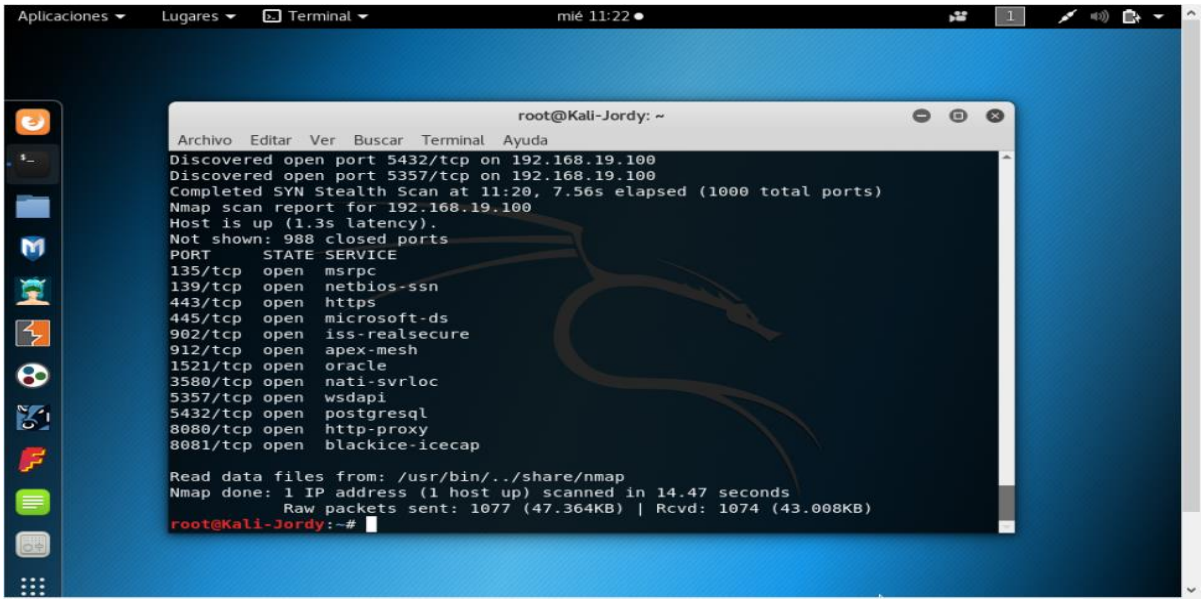

Figura 2. *Análisis de puertos abiertos con Kali Linux.*
Elaborado por: *Yordy Chonana Sosa*

Lo que dio como resultado los puertos abiertos en dicho equipo con el respectivo servicio que ejecuta.

De igual manera con otra IP tomada (192.168.26.151), podemos evidenciar los puertos abiertos que tiene este equipo.

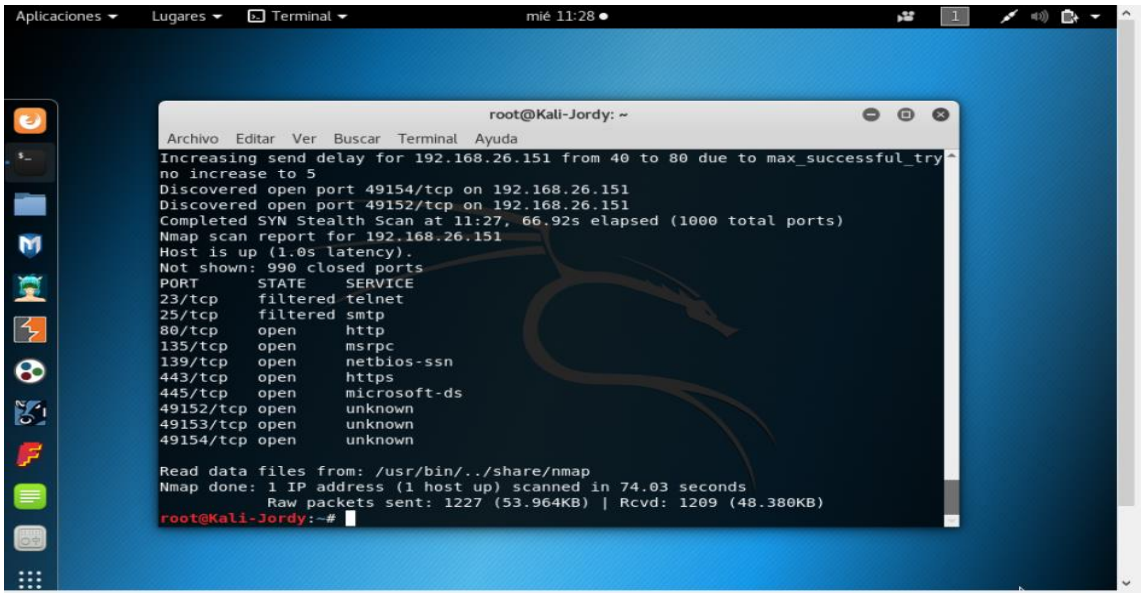

Figura 3. *Análisis de puertos abiertos con Nmap en la ip 192.168.26.151.*
Elaborado por: *Yordy Chonana Sosa*

Al realizar el mismo testeo de puerto con el escáner de vulnerabilidades Nessus se pudo evidenciar los siguientes resultados:

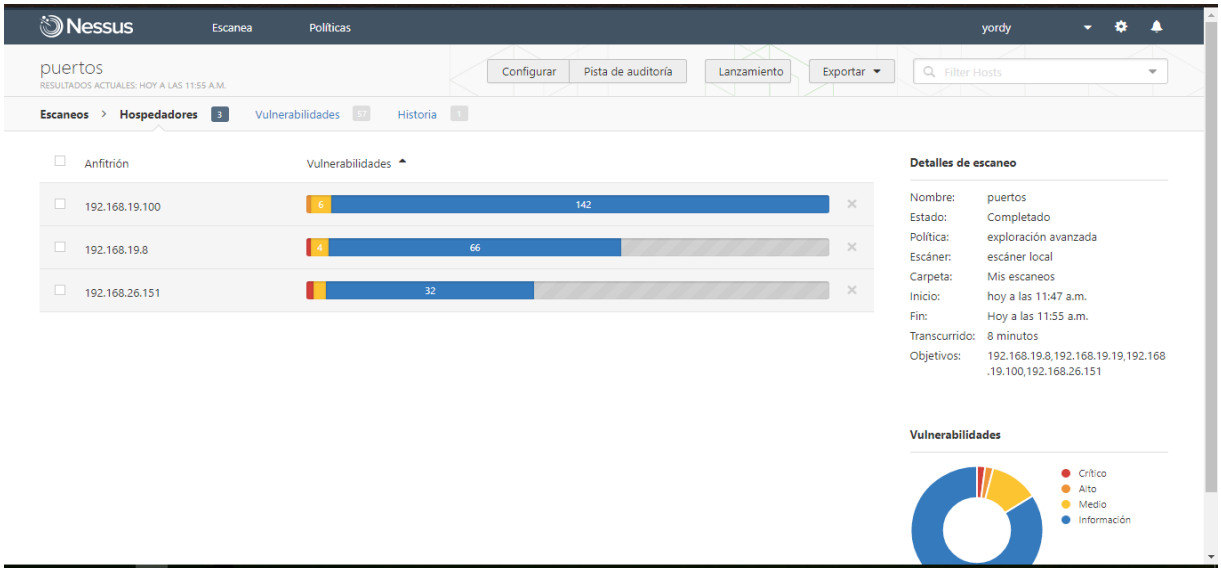

Figura 4. *Análisis de puertos abiertos con Nessus.*
Elaborado por: *Yordy Chonana Sosa*

Como se muestra en la imagen se hizo el análisis a las mismas IP con las que se realizó el escaneo en kali Linux y se agregó una más, dando como resultado el nivel de vulnerabilidades que tiene cada uno de estos equipos, tal como se muestra en la ***figura 5***.

Aquí tenemos un desglose del análisis.

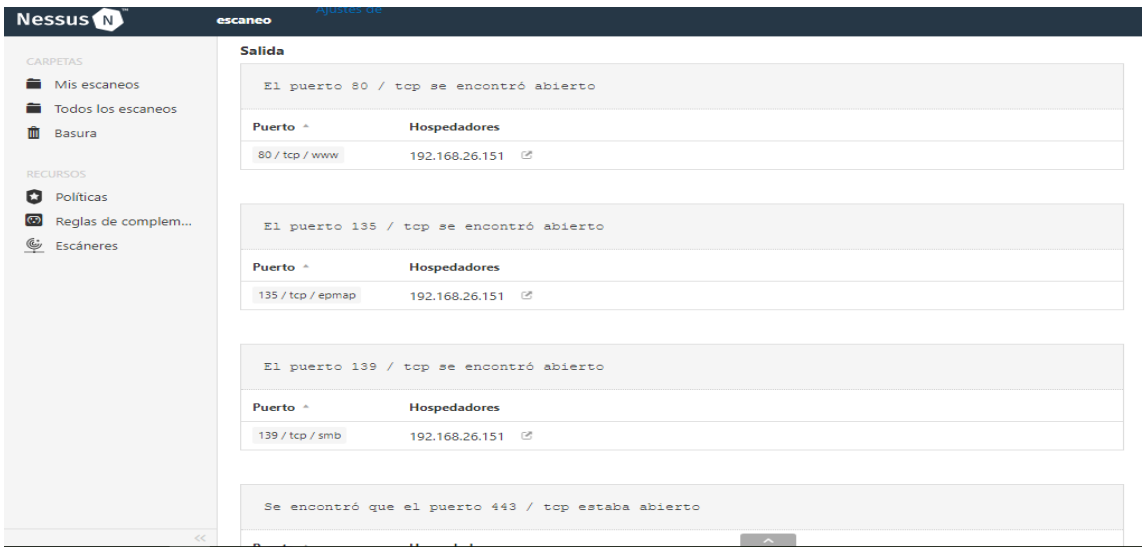

***Figura 5**. Resultado del análisis con Nessus (Puertos y características).*
***Elaborado por:** Yordy Chonana Sosa*

Una vez presentado el procedimiento del escaneo, da como resultado:

Puertos abiertos como: 80, 135, 139, 445, los cuales permiten filtraciones mal intencionadas, que pueden aprovechar estas entradas para realizar ataques a la red, tales como:

- **Denegación de Servicios (DoS**), que consiste en bombardear al servidor con peticiones para de esta manera dejarlo fuera de línea y de esta manera facilitar la infiltración (Raphael et al., 2015).
- **Recogida de Información**, en la que el atacante reúne una serie de información a través de herramientas que le permiten conocer IP, servicios de equipos, sistemas operativos, etc (Camacho, 2013).
- **Ataque de Sniffer**, consiste en captar la información que se transmite en una red de datos y de esta manera buscar su propio beneficio a través de aquella información. (Chicano, 2014), la define como "aplicaciones cuya función es obtener la información que envían los distintos equipos de una red" (p. 12).

El escaneo se lo realizo con dos herramientas muy conocidas y utilizadas para dar seguridad a los sistemas, en las cuales se pudo evidenciar el mismo resultado, lo que permite establecer la seriedad del escaneo.

Es decir, el peligro es eminente ya que cualquier persona mal intencionada podría explotar estas vulnerabilidades para poder manipular el sistema y de esta manera plagiar información de la institución, e incluso realizar ataques **man in the midle** el cual "consiste en que el atacante se sitúa entre dos equipos conectados en la red los cuales están estableciendo una comunicación, de tal manera que capta los datos transmitidos en ese momento, con el fin de

recuperar o alterar la información y luego los reenvía a su destino sin que ninguno de los dos actores legítimos de la comunicación se den cuenta" (Carpentier, 2016).

Por otra parte existe otro tipo de ataque conocido como "Retransmisión SMB", que hace uso de este protocolo de intercambio de archivos (SMB) y a través de un programa conocido como SMBRelay, retransmite los datos enviados entre el servidor y el cliente de tal manera que los modifica (Eset, 2017).

III. Conclusiones

Con el desarrollo de este estudio en el departamento de sistemas se ha podido evidenciar que aún existen vulnerabilidades en la red más que todo en los equipos, debido a la falta de parches en el sistema operativo que utilizan (Windows 7), es recomendable mitigar esta vulnerabilidad actualizando el sistema operativo a la última versión debido a que esta contiene todos los parches necesarios para contrarrestar aquellas vulnerabilidades.

Por otra parte, es se debe realizar un monitoreo constante a la red, de tal manera que se pueda identificar a tiempo posibles filtraciones de terceros, ya que como se vio en el resultado del escaneo existen puertos abiertos como el 139 y 445 que son usados para realizar ataques a equipos remotamente, Además, mantener desactualizado el software que utilizan presenta una vulnerabilidad, por tal motivo es recomendable mantener actualizados tanto navegadores, S.O, e incluso utilizar las famosas VPN (Redes Privadas Virtuales), además cerrar los puertos que no utilizan y proteger los que por el uso permanecen abiertos.

Referencias

Administracion, G. y. (s.f.). Gestion y Administracion. Recuperado el 17 de 11 de 2017, de Gestion y Administracion: https://www.gestionyadministracion.com/auditoria/auditoria-de-sistemas.html

Andres, R. (03 de 04 de 2016). Qué es Kali Linux y qué puedes hacer con él. Obtenido de Computer hoy.com: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671

Baca, U. G. (2016). Introducción a la seguridad informática. Recuperado de: https://ebookcentral.proquest.com

calder, A. (2017). Una vision de conjunto para la aplicacion de la ISO 2700:2013. Reino Unido: IT Governance Publishing.

Camacho, M. (09 de 01 de 2013). Hacking Etico. Obtenido de Information Gathering: https://hacking-etico.com/tag/seguridad-information-gathering-recoleccion-de-informacion-ataques/

Carpentier, J.F.(2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Recuperado de: https://books.google.com.ec/books?id=LKE5_6gzBmgC&pg=PA386&dq=ataque+man+in+the+middle&hl=es&sa=X&ved=0ahUKEwiMqbuyzv3YAhXldd8KHf76C3MQ6AEIRjAF#v=onepage&q=ataque%20man%20in%20the%20middle&f=false

Castro, M., Díaz G., Alzórriz I.y Sancristóbal E. (2014). Procesos y Herramientas para la seguridad de Redes. Madrid: UNED.

Chicano, E.(2015).Auditoria de Seguridad Informática.Recuperado de: https://books.google.com.ec/books?id=8a3KCQAAQBAJ&printsec=frontcover&dq=seguridad+informatica&hl=es&sa=X&ved=0ahUKEwiVmMmXgfbYAhUL7VMKHVwiD2UQ6AEIOjAE#v=onepage&q&f=false

Chicano, T. E. (2014). Gestión de incidentes de seguridad informática (mf0488_3). Recuperado de: https://ebookcentral.proquest.com

Escrivá, G. G., Romero, S., Ramada, J., Onrubia, R. (2013). Seguridad informática. Madrid: Macmillan.

Gallego, J. C. (2015). FPB - Instalcion y mantenimiento de redes para transmision de datos. España: Editex.

García, R. J. (2015). Creación de páginas web con contenido multimedia utilizando joomla 3.3. Recuperado de: https://ebookcentral.proquest.com

Ireo. (s.f). Ireo. Obtenido de Ireo: http://www.ireo.com/fabricantes-y-productos/sophos/sophos-utm/funcionalidades/

Rault, R.,Schalkwijk, L.,Crocfer, N., Crocfer, R., Dumas, D., y otros.(2015). Seguridad informática - Hacking Ético.Recuperado de: https://books.google.com.ec/books?id=4X32wbgtNfUC&printsec=copyright&hl=es&source=gbs_pub_info_r#v=onepage&q&f=false

Tropicode. (2017). Seguridad informática: Tipos de amenazas. [Entrada de Blog] Recuperado de: http://tropicode.net/seguridad/seguridad-informatica-tipos-de-amenazas/

Eset. (2017). Tipos de ataques remotos. Recuperado de: https://soporte.eset-la.com/kb2907/

Anexos

Análisis FODA

DEBILIDADES	FORTALEZAS
• Falta de Auditorias programadas. • Escasos recurso o poca inversión con respecto a infraestructura de los equipos. • Falta de generador eléctrico que alimente el servicio en caso de corte eléctrico.	• Existe personal con conocimientos de redes. • Se pueden detectar las anomalías en la red de datos. • Puede generar cambios significativos en el funcionamiento de la red de comunicación.
AMENAZAS	**OPORTUNIDADES**
• Cortes inesperados de electricidad. • Espacio reducido, para mantener los equipos de la red de comunicación. • Escasos métodos de seguridad en la red de datos.	• Capacitaciones en tecnología e infraestructura de red. • Implementación de estándares de calidad y control de los sistemas y equipos. • Aumento de la tecnología y la aparición de nuevos recursos con buena eficiencia y bajos costos.

Elaborado por: *Yordy Chonana Sosa*

Árbol de problema

Elaborado por: Yordy Chonana