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 INGENIERO EN SISTEMAS

TEMA:

Detección de vulnerabilidades en la red de datos de la Unidad Educativa "Jaime Roldós Aguilera"

EGRESADO:

Jonny Xavier Recalde Fierro

TUTORA:

ING. Narcisa Crespo Torres, MSC

AÑO 2018

I. INTRODUCCIÓN

Las unidades educativas públicas del Ecuador son lugares donde los docentes de Educación Básica y Bachillerato imparten clases a los estudiantes, pero además utilizan la red de datos para realizar actividades académicas que requieran el uso de la misma.

El presente trabajo de investigación tiene como objetivo determinar las vulnerabilidades que se presenten en la red de datos de la institución y que causen problemas de seguridad para la información que se maneja a través de dicha red. El utilizar una red que no sea de confianza o que no brinde la seguridad necesaria puede hacer que la información que se transmite sea vulnerable.

"Todo activo informático de una organización está en peligro de ser robado o manipulado poniendo en riesgo su integridad cuando se encuentra vulnerable, cuando se lleva a cabo un ataque informático y la seguridad presenta falencias pueden ocurrir pérdidas totales de información o ser alterada la confidencialidad e integridad de los datos." (Noticias de Seguridad Informática, 2016)

Debido a esto toda institución educativa que presta este servicio, tiene que asegurar que la información transmitida por este medio no sea accesible ni manipulada por personas que no estén autorizadas.

Frente a este problema se plantean las siguientes preguntas:

- ¿Qué medidas de seguridad tienen actualmente la red?
- ¿Existe algún método de autenticación para conectarse a la red?
- ¿De qué manera se protegen los equipos informáticos que componen la red de datos?

El presente trabajo de investigación tiene como objetivo determinar las vulnerabilidades que se presenten en la red de datos de la Institución y que causen problemas de seguridad para la información que se maneja a través de dicha red.

Estos serán estudiados desde el punto de vista informático obteniendo de esta manera un objetivo general, al igual que sus respetivos objetivos específicos:

- Averiguar el nivel de seguridad de la red.
- Examinar las medidas de seguridad que se encuentran implementadas para mantener un buen nivel de integridad de los datos de la institución educativa.
- Comprobar que la conexión de la red sea estable y permita que la conexión pueda realizarse sin problema.

Las limitaciones del presente caso determinan que su objeto de estudio es: La determinación de medidas de seguridad de los datos en la red de la institución educativa, el control de acceso a los equipos y verificación si los equipos de dicha red están configurados correctamente.

II. DESARROLLO

Una red de área local o LAN (Local Área Network) es una red de ordenadores que tiene un despliegue físico limitado a una habitación, un edificio o un conjunto de edificios, es decir, cubriendo un área relativamente pequeña y siempre dentro de una empresa o institución. Este tipo de redes se utiliza, sobre todo, para interconectar ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc. Al estar conectados entre sí, este tipo de redes es ideal para compartir recursos e intercambiar. (Paraninfo, 2014)

Actualmente las redes de datos en forma general manejan una cantidad de información prácticamente ilimitada, resultando esto en que los usuarios tienen acceso a información sobre vulnerabilidades motivo por el cual tienen cada vez más experiencia y permite que cada vez más personas las conozcan, esto vuelve a las redes cada vez menos seguras y más vulnerables a robos de información o ataques que pueden inhabilitar la red.

Una red de datos se considera insegura cuando la privacidad de los datos es muy limitada poniéndolos en riesgo de ser, interceptados, robados o alterados, también cuando son infectadas de virus que pueden dañar la información o los sistemas operativos ocasionando que la red no se encuentre funcionando en estado óptimo y se vuelva inestable, para evitar esto es necesario contar con equipos que brinden una seguridad y confiabilidad tanto en los datos como en el acceso al internet.

La seguridad en redes se considera en dos aspectos: física y lógica. En la primera se debe estar atento y tomar medidas preventivas como son los desastres naturales, inundaciones, terremotos incendios, así como también de las instalaciones eléctricas, etc. En la segunda se debe tener cuidado con aquellas personas que no están autorizadas para el acceso de la información, y es aquí donde entran los piratas de informáticos, un ejemplo de ellos son los hackers, crackers, etc. Que buscan algo que les interesa y después puedan poseerlo, o también para probarse a sí mismos hasta donde pueden llegar, aprovechándose de las vulnerabilidades de la víctima, como por ejemplo de los sistemas operativos o de la ingenuidad de los trabajadores al recibir archivos desconocidos y abrirlos, infectando el sistema por medio de virus u otra especie de herramientas. (Universidad de San Carlos, 2014)

Las principales amenazas las podemos clasificar en:

AMENAZAS FÍSICAS	AMENAZAS LÓGICAS
Desastres naturales. Fallos en los suministros (energía, internet, equipos). Robos de información.	Pérdida de datos. Virus informáticos, malware, troyanos. Ataques e intrusiones a la red.

Tabla 1.”Principales amenazas de una red de datos”

Fuente: Elaborado por Jonny Recalde

La Universidad de Luján define las amenazas como: “cualquier mecanismo o tarea preparada para de infringir y vulnerar contra la seguridad de los activos informáticos. Estos riesgos nacen desde que exista una vulnerabilidad que pueda ser explotada, no es necesario que la seguridad de una red sea totalmente vulnerable, basta con que exista un pequeño agujero que permita filtrar la información confidencial, además se puede vulnerar por medio de la ingeniería social, esto debido a últimamente se ha incrementado significativamente este tipo de ataques por la falta de instrucción y concientización necesaria en los usuarios, también un motivo muy importante es el benéfico que pueden obtener con la información robada, todos estos motivos han inducido en los años actuales años el incremento de este tipo de ataques”. (Luján, 2017)

Dentro de una unidad educativa de educación básica y bachillerato es indispensable contar con una red de datos que permita manejar información importante tanto de manera local como a través del internet para ello deben contara con los equipos necesarios para que esto sea posible con un nivel óptimo de seguridad de la información.

Según un análisis en SlideShare: “Los productos más utilizados de la web son: correos, inteligencia de negocios y la nube. Las tecnologías de la información y la comunicación (TIC) han logrado una gran notabilidad, especialmente al volverse el uso de internet en el ámbito educativo algo tan trascendental como necesario para lograr para ampliar los horizontes de la educación.” (adrisurio, 2016)

Si describimos el contexto internacional podemos tomar como referencia a Norteamérica, donde el uso de las TIC`s en el ámbito educativo es indispensable para el desarrollo y la formación profesional. Esto brinda grandes beneficios en la capacitación de los estudiantes y maestros con la comunicación por medio de computadoras, cursos online, video conferencia, aulas virtuales, etc.

En el ámbito nacional se puede decir que la gran mayoría de instituciones de educación básica y bachillerato cuentan con una red de datos y con acceso a internet.

El Proyecto Dotación de Conectividad y Equipamiento, que impulsa el Ministerio de Telecomunicaciones y de la Sociedad de la Información (Mintel), beneficia a 7.000 colegios y escuelas fiscales del Ecuador. El proyecto dota de equipamiento tecnológico y acceso a Internet a los estudiantes de las instituciones educativas públicas, con el objetivo de mejorar la enseñanza de los jóvenes y niños del Ecuador. Con el Gobierno de la Revolución Ciudadana se adoptaron políticas de inclusión digital a nivel escolar para llegar con equipamiento y conectividad a las zonas más alejadas del país. Hasta el momento, el Mintel intervino en 7.000 instituciones educativas, lo que evidencia el desarrollo de la educación en el país. (El Ciudadano, 2015)

Debido a esto y tomando en cuenta la información antes mencionada es necesario que todas estas instituciones educativas cuenten con la respectiva seguridad de los datos y el acceso a internet que brinde la seguridad a todos los usuarios, en este caso específico se realizara la detección vulnerabilidades de la Unidad Educativa Jaime Roldós Aguilera del Cantón Montalvo.

La Unidad Educativa tiene acceso a internet, cuenta con un laboratorio informático con 30 computadores conectados al internet además de que en cada oficina cuenta con un computador también con acceso al internet. Estos equipos brindan acceso a las diferentes plataformas educativas que utilizan los docentes así como también el laboratorio es utilizado por los estudiantes de las diferentes aulas para el aprendizaje.

Si se especifica la conexión de la red de datos es necesario contar con los equipos necesarios para dicha conexión como es routers, switch, cable par trenzado, fibra óptica, etc.

"Se conoce como router a el dispositivo que permite conectar diferentes ordenadores de una red LAN y permite que estas intercambien datos o información así como también compartir la misma conexión de internet, este artefacto trabaja en la capa tres del modelo OSI, la misma que consta de un equipo origen y otro destino, estos se encuentran ligados o conectados por medio del Router". (ValorTop S.L., 2015)

Podemos resumir que el router es un dispositivo de hardware concebido para permitir la conexión de varios ordenadores de la misma red y que permite la interconexión con otra red. Opera en la capa tres del modelo OSI.

"El modelo **OSI (Open Systems Interconnection o Interconexión de Sistemas Abiertos)** es una organización *desarrollada en los años80* por la *Organización Internacional de Estándares (ISO)* con el propósito de implantar una pauta en el desarrollo de protocolos de comunicación. Estas reglas se rigen a un estándar que provee un marco referencial, por lo tanto resumidamente el modelo OSI es un estándar de estándares." (Solvetic, 2014)

En pocas palabras la información es trasmitida verticalmente por medio de las 7 capas que componen el modelo OSI, las mismas que describen todos los procesos que se deben realizar para que la comunicación funcione a través de la red.

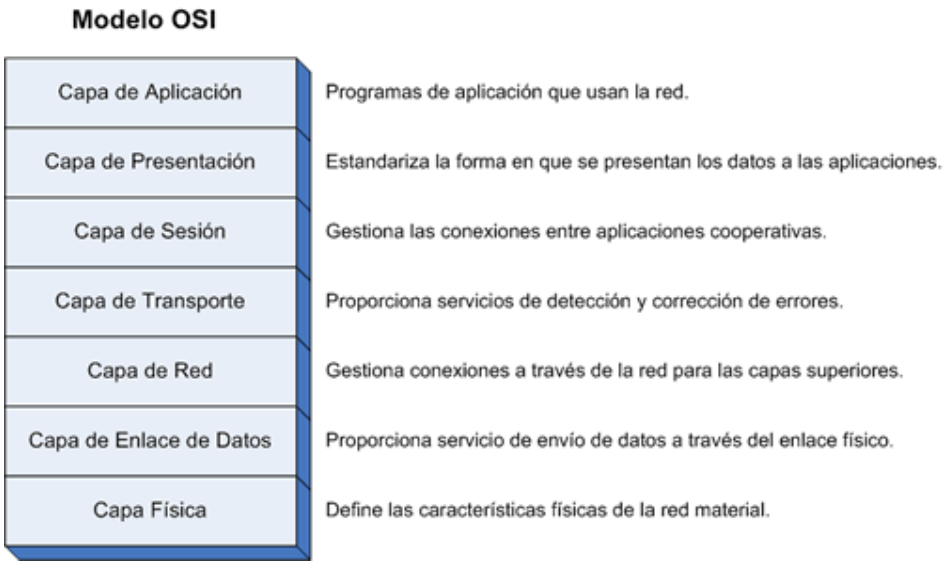

Figura 1. "Capas del Modelo OSI"

Fuente: (TextosCientificos.com, n.d.)

"Switch es un aparato electrónico que permite la conexión de varios equipos dentro de una misma red. Estos pueden ser un PC, una impresora, la misma televisión, tu consola preferida o cualquier aparato que posea una tarjeta de red." (About Español, 2017)

El switch se encarga de la retransmisión de la información solo por el puerto donde se encuentra el objetivo, para esto utiliza la dirección MAC (Media Access Control) que son direcciones físicas de la tarjeta de red.

Si se conectan varios switch se comunican entre ellos para saber hacia dónde se debe enviar la información, es un dispositivo diseñado para facilitar la comunicación entre equipos de una misma red.

"Si bien un switch y un router tienen similitudes en su funcionamiento hay grandes diferencias, por lo que son utilizados cada uno para un fin específico dentro de una red, un router posee características que admiten conectarse a redes más grandes. Es común ver router ADSL, o router de fibra en relación a la red que después te conecta a Internet. Para realizar su labor un router trabaja con direcciones IP mientras un switch opera con direcciones MAC. Las direcciones MAC se usan solo en una red LAN, mientras las IP pueden usarse para identificar un ordenador dentro de la red local como también en la internet." (About Español, 2017)

Cable Par trenzado es el método de conexión más común dentro de una red de área local, tiene una forma en la que sus cables están trenzados en pares para tener menor interferencia y aumentar la potencia de trasmisión.

Según el (Cuerpo de Profesores Técnicos, 2006): "El cable par trenzado está formado por pares de hilos con una cubierta protectora de plástico formando una trenza a lo largo de su recorrido. Tiene un grosor de entre 0,6 y 1,2 milímetros y se trenza para reducir la diafonía. La

longitud de la trenza está comprendida entre los 5 y 15 centímetros, presentan un ancho de banda estrecho y es muy susceptible a interferencias, factores que limitan la velocidad del mismo".

"Se conoce como fibra óptica a unos hilos de vidrio (o plástico) que tienen la capacidad de conducir la luz. En la actualidad, es ampliamente utilizada en las comunicaciones ya que, comparada con el tradicional cable eléctrico, permite la trasmisión de una gran cantidad de datos a largas distancias. El primer uso que se le dio a la fibra óptica fue para la trasmisión de imágenes que, en la actualidad, se sigue utilizando en los endoscopios. Debido a sus diferentes propiedades, la fibra óptica también es utilizada para la iluminación, en láseres y para sensores." (EL Mundo, 2015)

El problema de la red de datos en la institución se definirá en función a la observación, elaboración de entrevistas con la persona encargada de administración de la red.

El **objetivo principal** de esta investigación es detectar las vulnerabilidades de la red de datos de la Unidad Educativa.

Como objetivos específicos tenemos:

- Realizar una evaluación visual de las estructura de la red en busca de vulnerabilidades físicas.
- Evaluar las configuraciones de los equipos informáticos para determinar vulnerabilidades que puedan comprometer la información.
- Realizar una encuesta al administrador de la red para conocer el nivel de conocimiento que tiene sobre la seguridad de la información.

Como justificación, este proyecto que tiene como finalidad contribuir al fortalecimiento de un ámbito tan importante como es la seguridad en las redes, demostrando a través de un análisis si existen vulnerabilidades tanto en el acceso a la red como en la manera que se transmiten los datos a través de ella.

Una vez que se ha evaluado la seguridad de la red, se determinaran el tipo de vulnerabilidades que se hayan encontrado; así la investigación se encamina a realizar reportes de fallas encontradas y ya su vez sugerir un conjunto de recomendaciones que puedan garantizar una seguridad aceptable en este tipo de redes.

Junto con la utilización de los Métodos Teóricos Investigativos y el conocimiento empírico que serán de ayuda para generar un criterio de manejo de la investigación, en base a la recopilación, análisis y clasificación de toda la información relacionada con las diferentes tecnologías, métodos y herramientas involucradas en el proyecto.

El método inductivo se aplica, debido a que al observar los parámetros de configuración para evaluar la red enmarcada dentro de los procedimientos, se va a llegar a una propuesta que permita ofrecer una guía referencial de mejores prácticas para mantener un buen nivel de seguridad.

Entre las técnicas que vamos a utilizar tenemos:

Observación

Observar el perímetro donde se encuentran instalados los diferentes equipos de la red, así como su nivel de seguridad frente a las diferentes amenazas que se pueden presentar.

Experimentación

Se experimentará sobre los equipos analizando la configuración de ellos para verificar su nivel de seguridad y vulnerabilidades que puedan presentar.

Entrevistas

Entrevista al administrador, para obtener diferentes puntos de vista y enfocarse en ideas de experiencias profesionales.

Beneficios del análisis de la red en busca de vulnerabilidades.

Son varios los beneficios que ofrecen la realización de este caso ya que nos permite establecer el nivel de inseguridad y vulnerabilidades de la red, realizando este estudio con previa autorización de los directivos de la institución.

Entre las principales tenemos:

- Conocer el nivel de vulnerabilidad.
- Reducir los riesgos que pueden generar pérdidas o robo de información confidencial de la institución.
- Ahorrar tiempo y dinero al corregir situaciones nefastas antes de que ocurran y obliguen afrontar costos más grandes.
- Mejorar la imagen y de la institución educativa permitiendo garantizar la confidencialidad de la información que se maneja a través de la red.

Factibilidad Operativa: Este análisis de vulnerabilidades en la seguridad será realizada especialmente para incrementar la seguridad de la red.

Factibilidad económica: Tomando en consideración que no se necesitara más que el tiempo de la persona que realizara el análisis con la disponibilidad del acceso a la infraestructura, esto no generará un costo significativo para la persona encargada de su ejecución.

El análisis de factibilidad nos demuestra que el proyecto es viable y su realización no requeriría una gran inversión económica y la tecnología necesaria está al alcance de todos, por lo tanto esto no representa ningún impedimento para su desarrollo.

A continuación se detalla las características que tiene esta infraestructura de red:

Usuarios: aproximadamente a la red de la institución acceden diariamente más de 200 usuarios, este personal es de tipo administrativo, docentes y estudiantes.

Los servicios que acceden a través de la red inalámbrica son principalmente: Internet, plataformas educativas como también las diferentes aplicaciones que son utilizadas para la enseñanza.

Los portales web a los que acceden a través de la red son: Portales del Ministerio de Educación (MINEDUC), Correos personales, Portal Educativo Educar Ecuador, Entre otros.

Con el fin de facilitar el análisis de la red será descrita basados en el modelo jerárquico de red de la academia CISCO.

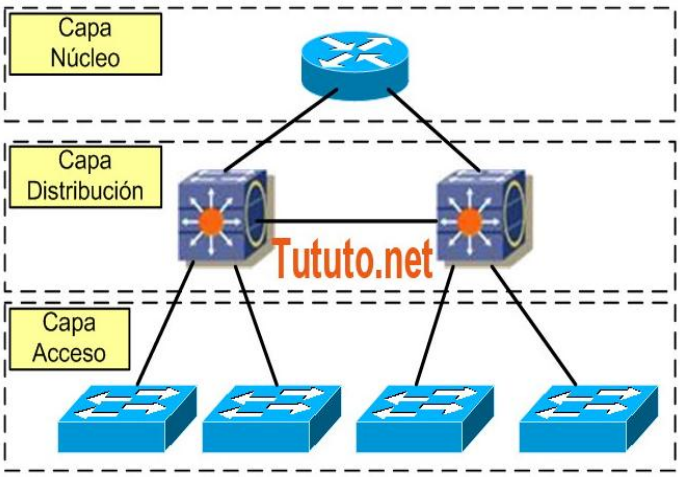

Figura 2. "Capas de red, modelo jerárquico CISCO"

Fuente: (TUTUTO.NET, 2015)

“El Modelo jerárquico Cisco propone tres capas en el diseño de redes. La ventaja de este diseño es que a pesar que los equipos que componen cada capa están interconectados, son independientes en cuanto a funcionamiento, que nos ayudan en gran medida en la detección de problemas.” (TUTUTO.NET, 2015)

Este modelo brinda muchos beneficios en el diseño de una red, entre los más importantes es que al separarla en 3 niveles su diseño es más fácil, además al tener un diseño escalar aumenta su confiabilidad, con una mejor relación costo/beneficio.

La **capa de acceso** es la que se encarga de controlar a los usuarios y grupos de trabajo administrando los recursos.

La **capa de distribución** permite la comunicación entre la capa de acceso y la capa núcleo, administrando el ruteo, filtrado y acceso a la red.

La **capa núcleo** como su nombre lo indica, es el núcleo de la red, su función es transmitir el tráfico de la red con la mayor velocidad posible, administra gran cantidad de información de manera eficiente.

En las siguientes tablas se describen los equipos y dispositivos de la infraestructura de red de la institución la cual ha sido clasificada en equipos cliente y equipos de red:

EQUIPOS CLIENTE				
CANTIDAD	**ACTIVO**	**CARACTERÍSTICAS**	**FUNCIÓN**	**OBSERVACIÓN**
35	Ordenadores	N/A	Terminales de mesa con acceso a la red cableada.	Computadores de escritorio.
10	Portátiles	N/A	Terminales móviles que pueden tener acceso tanto a la red cableada como a la red inalámbrica	

Tabla 2. "Activos de clientes o usuarios"

Fuente: Elaborado por Jonny Recalde

EQUIPOS DE RED				
CANTIDAD	**ACTIVO**	**MODELOS**	**FUNCIÓN**	**OBSERVACIÓN**
1	Router	Marca: Microtick Routerboard RB750GL	Este dispositivo está en la capa Núcleo del modelo jerárquico de la red.	Computadores de escritorio.
3	Switch	Marca: Tplink SG-1016D	Para la capa de distribución del modelo jerárquico de la red.	No requiere configuración.

Tabla 3. "Equipos de la red de la institución"

Fuente: Elaborado por Jonny Recalde

Para comprobar el nivel de seguridad del router se utiliza el software *Zenmap 7.60* con el fin de conocer los puertos habilitados en el router.

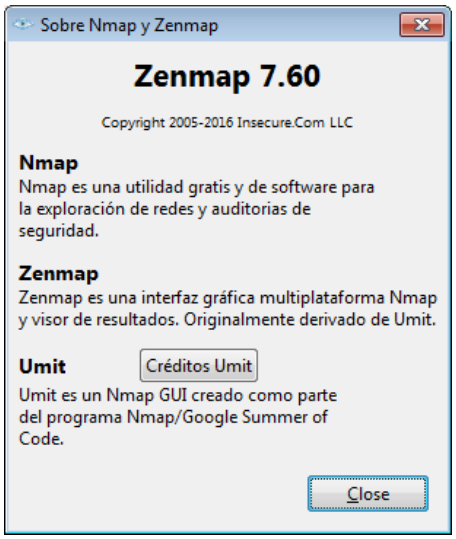

Figura 3. "Detalles de aplicación Zenmap"

Fuente: Elaborado por Jonny Recalde

Para realizar el escaneo se ingresa la dirección ip del router y se elige el tipo de escaneo que se desea realizar, en este caso se desea realizar un escaneo intenso.

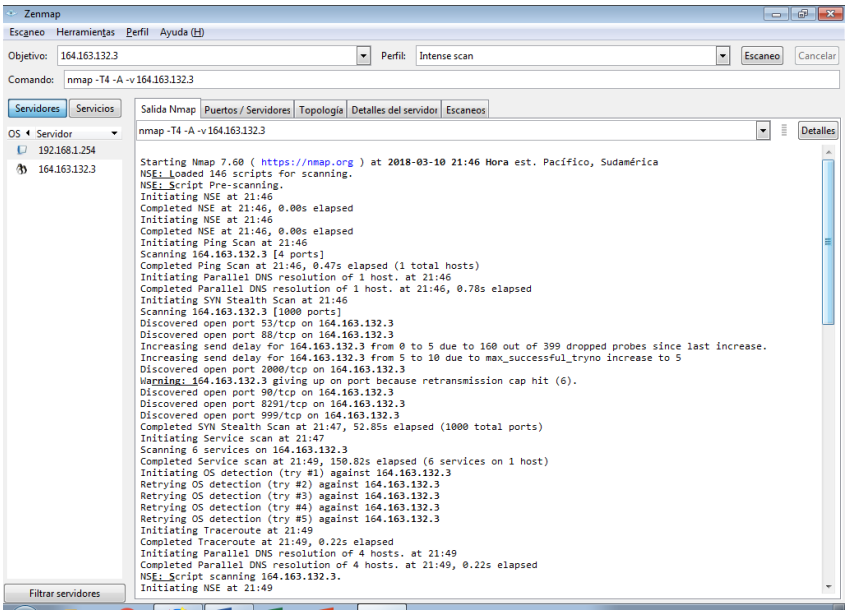

Figura 4. "Escaneo de puertos del Router"

Fuente: Elaborado por Jonny Recalde

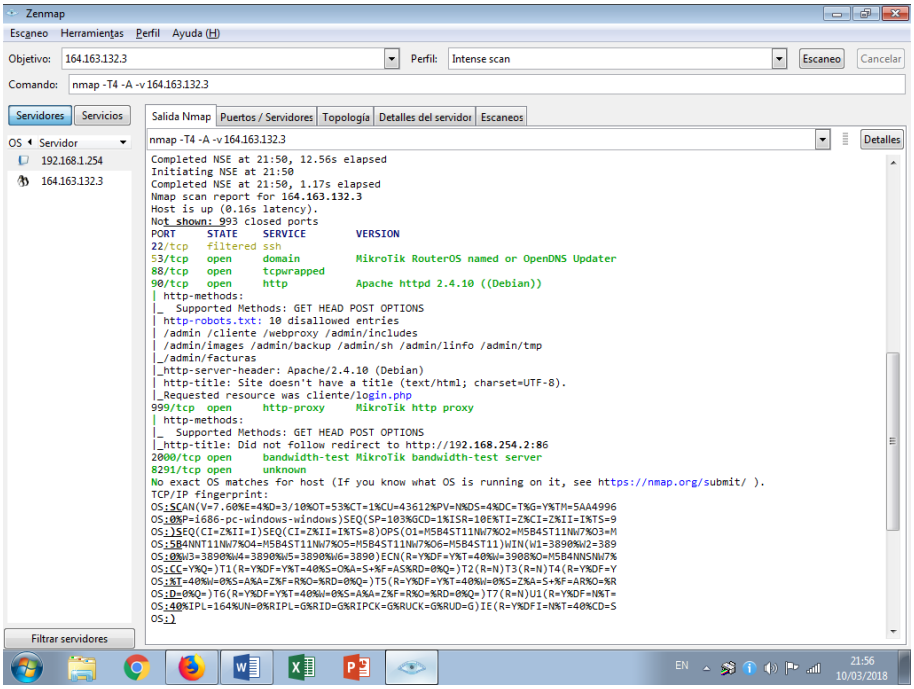

Figura 5. "Resultados del escaneo"

Fuente: Elaborado por Jonny Recalde

Además con el fin de examinar la configuración del router se utilizara el software **Winbox**.

"Winbox es una pequeña utilidad que te permite la administración de **Mikrotik RouterOs** usando una interfaz gráfica de usuario fácil y simple. Se lo puede descargar directamente desde el Router." (Anrrango, 2015)

Para conectarse al Router se ingresa la dirección Ip del mismo seguido del usuario y clave de acceso:

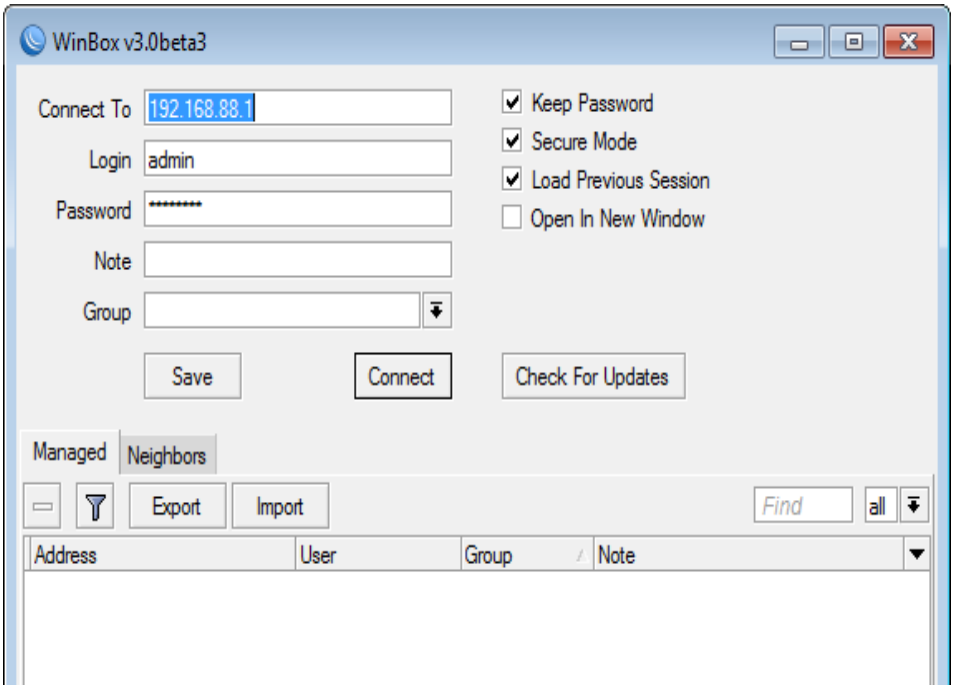

Figura 6. "Acceso al Router"

Fuente: Elaborado por Jonny Recalde

Se procede a revisar la configuración de la interfaz Ethernet:

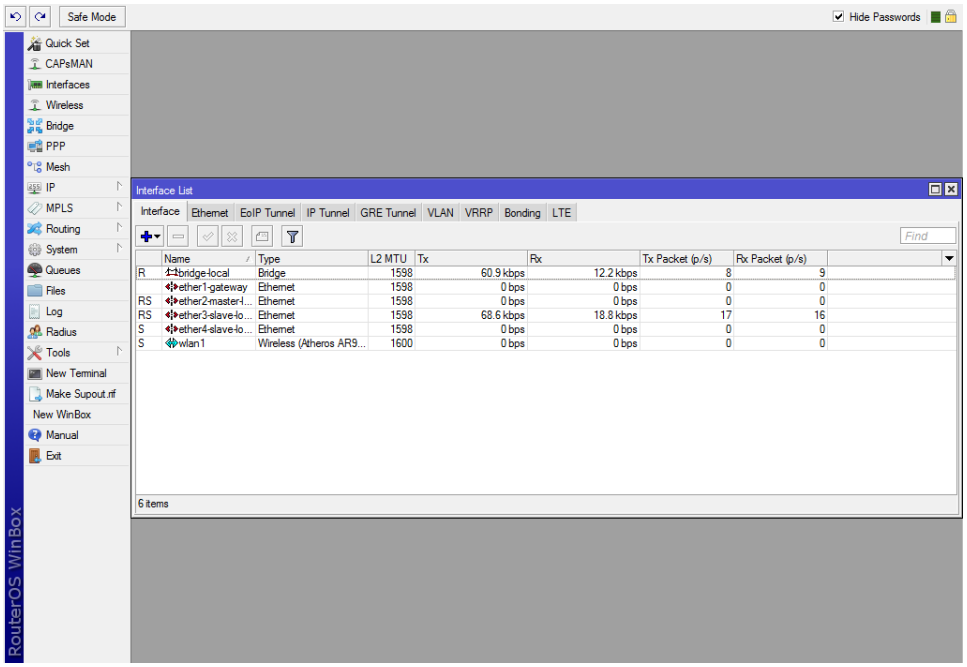

Figura 7. "Configuración Ethernet"

Fuente: Elaborado por Jonny Recalde

Revisamos la interfaz de la red inalámbrica donde nos damos cuenta que no se ha realizado ningún cambio a de la configuración que trae por defecto:

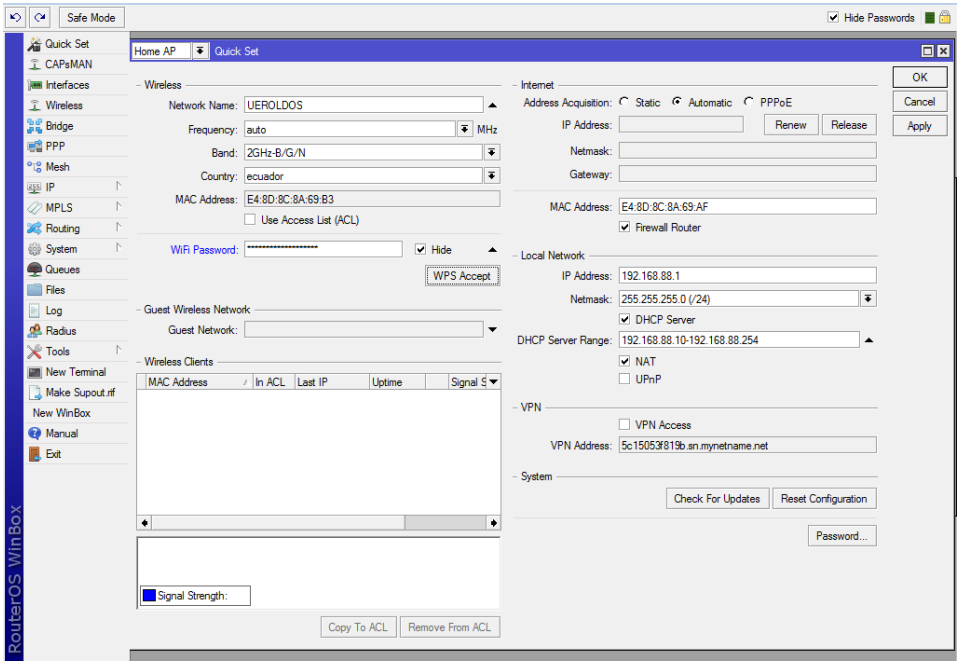

Figura 8. "Configuración de red inalámbrica"

Fuente: Elaborado por Jonny Recalde

Los problemas de seguridad que se han encontrado en la red de la institución:

Políticas de seguridad

La institución no cuenta con políticas de usuarios o un conjunto de buenas prácticas para el uso de la red. Es decir que no puede garantizar el buen manejo de servicios y recursos de la red, ni que las operaciones las realicen solo usuarios autorizados.

No se realizan capacitaciones periódicas al personal; debido a esto existe un desconocimiento en cuanto a metodologías o herramientas que un hacker podría utilizar para tener acceso a la información sensible a través de la misma.

Administración de los dispositivos

La institución no cuenta con un inventario completo de todos los dispositivos y no realizan actualizaciones de los últimos parches. Tampoco se conoce de las limitaciones en el hardware y software que pueden tener los equipos. Es decir, los dispositivos no se encuentran dentro de un marco planificado por lo que su configuración pone en peligro la seguridad.

Control de acceso

Los controles de acceso físico a los equipos informáticos que tiene la institución no garantizan seguridad perimetral. Se desconoce si existen interferencias con otros dispositivos electrónicos que tengan frecuencias similares o si la comunicación inalámbrica se extiende más de los límites físicos de la institución.

Para los usuarios que ya están dentro de la red, no presenta ninguna distinción de parámetros o accesos diferenciados entre grupos de usuarios propios de la institución y visitantes.

Configuración de los dispositivos

A continuación se detallan los controles que hacen falta:

- La robustez en las contraseñas administrativas, el cambio periódico, la caducidad y el manejo de las mismas.
- Los clientes no cuentan con un Firewall y antivirus instalado en su última versión, por lo tanto no garantiza seguridad a la red inalámbrica.
- No todos los parámetros de configuración fueron cambiados y se encuentran ciertas configuraciones con los predeterminados que vienen en el dispositivo. Eso indica que están habilitados protocolos de gestión insegura e innecesaria en los dispositivos.

CONCLUSIONES

- Muchas de las vulnerabilidades encontradas en la red no se deben al mal funcionamiento de los dispositivos sino más bien a su mala configuración; esto debido a que en la mayoría de casos el personal desconoce sobre seguridad informática y los riesgos a los que puede estar expuesta la red al no contar con la seguridad respectiva.

- A pesar de todo esto se ha podido observar que el personal tanto administrativo como técnico tiene toda la voluntad de brindar las facilidades pertinentes para solución de las vulnerabilidades encontradas.

- Se recomienda la capacitación necesaria del personal técnico y la implementación de políticas de seguridad que brinden un control de acceso a la red de la institución para de esta manera brindar la seguridad necesaria para los usuarios y mantener a salvo toda la información que se maneja dentro de la institución educativa.

BIBLIOGRAFÍA

About Español. (29 de Julio de 2017). *About Español*. Recuperado el 8 de Enero de 2018, de https://www.aboutespanol.com/que-es-un-switch-841388

adrisurio. (4 de Julio de 2016). *SildeShare*. Recuperado el 7 de Enero de 2018, de https://es.slideshare.net/adrisurio/la-importanciadeinternetenlaeducacin

Anrrango, R. (16 de Septiembre de 2015). *Mikrotik Wireless*. Recuperado el 29 de Enero de 2018, de http://configurarmikrotikwireless.com/blog/de-que-se-trata-winbox.html

Cuerpo de Profesores Técnicos, d. F. (2006). *Sistemas y Aplicaciones Informáticas.* Sevilla, España: MAD, S.L.

El Ciudadano. (16 de Noviembre de 2015). *El Ciudadano*. (V. Macias, Editor) Recuperado el 7 de Enero de 2018, de http://www.elciudadano.gob.ec/la-conectividad-escolar-llega-a-7-000-instituciones-educativas/

El Grupo Informático, (. (11 de Mayo de 2017). *El Grupo Informático*. Recuperado el 9 de Enero de 2018, de https://www.elgrupoinformatico.com/que-una-direccion-mac-t36266.html

EL Mundo. (18 de Marzo de 2015). *El Mundo*. Recuperado el 10 de Enero de 2018, de http://www.elmundo.es/economia/2015/03/18/55097356268e3e094f8b457a.html

Luján, U. d. (1 de Febrero de 2017). *Departamento de Seguridad Informática*. Recuperado el 05 de Febrero de 2018, de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Noticias de Seguridad Informática. (2 de Marzo de 2016). *Noticias de Seguridad Informática*. Recuperado el 29 de Diciembre de 2017, de http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

Paraninfo. (2014). *Redes locales.* Madrid, España: Ediciones Paraninfo, S.A. Recuperado el 5 de Enero de 2018

Solvetic. (2 de Julio de 2014). *Solvetic*. (MPachano, Editor) Recuperado el 7 de Enero de 2018, de https://www.solvetic.com/tutoriales/article/888-redes-%E2%80%93-el-modelo-osi/

TextosCientificos.com. (s.f.). Obtenido de https://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

TUTUTO.NET. (20 de Agosto de 2015). *TUTUTO.NET*. Recuperado el 28 de Enero de 2018, de http://tututo.net/modelo-jerarquico-cisco-redes-datos

Universidad de San Carlos. (2014). Seguridad de la Información. *Segunda Cohorte del Doctorado en Seguridad Estratégica*, 374. Recuperado el 5 de Enero de 2018

ValorTop S.L. (18 de Agosto de 2015). *ValorTop*. Recuperado el 7 de Enero de 2018, de http://www.valortop.com/blog/que-es-un-router-y-un-modem-en-que-se-diferencian

ANEXOS

ENCUESTA AL ADMINISTRADOR DE LA RED

PREGUNTAS

1. ¿Es consciente que al momento de conectarse a una red en caso de no poseer ningún tipo de seguridad en su computador otras personas pueden acceder a la información de la misma?

a. Si
b. No

2. ¿Es de su conocimiento la que la información que se transmite en una red es susceptible a que ésta pueda ser interceptada por otra persona?

a. Si
b. No

3. ¿Cree que se mantiene la confidencialidad de los datos en la red de la Unidad Educativa?

a. Si
b. No

4. ¿Ha sido víctima de robos de contraseñas al usar la red de la Unidad Educativa?

a. Si
b. No

5. ¿Qué tipo de seguridad poseen los ordenadores para evitar robos de información?

a. Firewall
b. Software de detección de malware
c. Software de detección de spyware
d. Antivirus
e. Ninguna

6. ¿Cuándo se desea acceder al internet está disponible?

a. Siempre
b. Tiene que esperar unos minutos para poder conectarse
c. Está disponible pero no conecta

7. ¿Cómo considera el nivel de velocidad de la red?

a. Rápido.
b. Normal.
c. Lento.

8. ¿Cómo considera el nivel actual de seguridad en la red?

a. Alta
b. Media
c. Baja