UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO - OCTUBRE 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ESTUDIO DE LA SEGURIDAD DE LA RED DE DATOS DEL GAD FEBRES CORDERO

EGRESADO:

MAURICIO FERNANDO CAMPI MARTÍNEZ

TUTORA:

ING. NARCISA CRESPO TORRES, MSc.

AÑO 2018

Introducción

El GADP (Gobierno Autónomo Descentralizado Parroquial) de Febres Cordero de la Provincia de Los Ríos cantón Babahoyo, es una institución con la finalidad de liderar, articular procesos de desarrollo en la parroquia, promueve y ejecuta Políticas Públicas con la finalidad de solucionar las necesidades a todos los moradores de la Parroquia.

Gobierno Autónomo Descentralizado Parroquial de Febres Cordero, tiene como misión lograr un alto desarrollo humano reduciendo la contaminación ambiental, conservando los ecosistemas existentes diversificando e implementando una economía sostenible , generando bienestar para un buen vivir en todas las familia, población de la Parroquia Febres Cordero incentivando, valores y principios.

El presente caso de estudio analizará las falencias en seguridad de la red de datos de la institución, en este sistema de datos constan de conectores, canalizaciones y dispositivos, que permite establecer un sistema de comunicación en una infraestructura de telecomunicaciones dentro del edificio. En una red de datos segura se debe tener siempre presente las características y estándares que se debe cumplir.

La Red de datos permite transportar dentro del edificio la información y señales que son enviados del emisor y recibidas por el o los receptores. En la red física se puede cambiar fácilmente los cables UTP, bloques de conexión, adaptadores entre otros elementos de la estructura del cableado. Al soportar diferentes dispositivos de telecomunicaciones, sin tener los mayores conocimientos sobres los productos que se utilizan sobre él.

Los trabajadores que intervengan en cualquier fase de la trasmisión de datos deben guardar el debido respeto de carácter profesional que pueda evitar su alteración o pérdida de paquetes de datos por posible riesgo de presencia de intrusos, en sus diferentes tipos, en la red, interferencias electromagnéticas y la eventual posibilidad de instalar redes virtuales.

La seguridad en una red de datos establece una serie de principios relativos al tratamiento y protección de datos, además deben conocerse muchos factores de la red de datos, está formada por un grupo de dispositivos interconectados entre sí, constituidas por las diferentes tecnologías de hardware, software y el departamento de telecomunicaciones que va directamente con el equipo de telecomunicaciones.

Desarrollo

El GADP (Gobierno Autónomo Descentralizado Parroquial) de Febres Cordero, es una institución sin fines de lucro, en la actualidad se encuentra un desafío muy grande que es servir a la población de la Parroquia Febres Cordero que cada vez es más exigente, en el que se contribuye con la formación de emprendedores con ideales de superación para que de esta manera contribuyan al desarrollo de la familia y la comunidad.

En la actualidad es muy importante que el GADP (Gobierno Autónomo Descentralizado Parroquial) de Febres Cordero, tenga una red de datos que brinde seguridad y confianza en la transmisión de paquetes de datos donde permita el ingreso de diversos servicios como de datos, voz y videos. Dando un servicio confiable en el envío, recepción de información y por ende la confiabilidad , satisfacción al personal administrativo y de servicio al momento de realizar las actividades asignadas.

La seguridad en la red de datos debe registrar, administrar el flujo de la información entre los diferentes dispositivos, pueden tomar uno o dos caminos está compuesto de elementos que permite la interconexión de equipos tecnológicos en organizaciones públicas o privadas, para lo cual se integran diferentes sistemas de control, comunicación, manejo y almacenamiento de la información, la implementación debe cumplir los estándares para que garanticen su capacidad de rendimiento y la confiabilidad.

Según (Gómez, 2012). Los complementos de seguridad, el router y los dispositivos físicos deben estar ubicados en un cuarto bajo llave el cual es accesible solo para personal autorizado, libe de interferencias electromagnética

y electroestática, además en las políticas de seguridad es recomendable generalizar un lenguaje de seguridad en toda la red.

Hoy en día la seguridad en las redes de datos son primordiales en el envío y recepción de información dentro de una empresa o institución, se puede decir que la red de datos nos facilita el cruce de información entre todos los sistema de telecomunicación existente.

Políticas de seguridad

La política de seguridad en redes traza las reglas de acceso a la red, determina como se harán cumplir las políticas y describen la arquitectura básica de un ambiente básico de seguridad.

Antes de crear una política de seguridad deben entenderse que servicios están disponibles, para que los usuarios en la seguridad de red es necesario establecer una jerarquía de permisos de acceso.

(Ernesto A. , 2014)

- ✓ Seguridad de red a un nivel superior
- ✓ La dimensión lugar donde se realizara el cableado.
- ✓ La cantidad de usuarios conectado a la red.

Evaluación de Riesgos

El primer paso en el proceso de administración de riesgo califica el valor de riesgo relacionado con las amenazas y situaciones.

- ✓ Políticas de seguridad
- ✓ Organización de la seguridad
- ✓ Administración de las comunicaciones

- ✓ Control de acceso
- ✓ Administración de incidentes
- ✓ Administración de la comunidad en la red

Imagen 1: Seguridad informática 2015
Fuente: http://seguridadinformaticamila.blogspot.com

En la imagen # 1 representa el tipo de seguridad que debe tener toda empresa sea pública o privada, estos son unos de los requisitos principales para salvaguardar y proteger la información de nuestra empresa.

Ventajas

- ✓ Integridad
- ✓ Confidencialidad
- ✓ Disponibilidad
- ✓ Autenticación

Desventajas

- ✓ Registro de teclas pulsadas
- ✓ Captura de formularios
- ✓ Capturas de pantalla y grabación de video
- ✓ Inyección de campos de formulario fraudulentos
- ✓ Inyección de páginas fraudulentas

- ✓ Redirección de páginas bancarias

Características de la seguridad informática (Urbina, 2016)

Muchos investigadores y autores especializados en el tema de seguridad informática por lo común se centran solo en las tres características de la información mencionadas; no obstante, de acuerdo con el marco de gestión y el marco global para la gestión de las TI(Tecnología Informática) de la empresa (COBIT por sus siglas en ingles), las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad, cada una de las cuales se describen a continuación. (Urbina, 2016)

1. **Efectividad.-** se trata de lograr que la información sea en realidad necesaria para desarrollar cualquiera de las tareas que se desarrollan en la empresa u organización y sea adecuada para realizar los procesos del negocio, proporcionándola de manera oportuna, correcta, consistente y accesible.
2. **Eficiencia.-** Significa que la información será generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin.
3. **Confidencialidad.-** Se refiere en que todas las etapas del procedimiento de la información, esta se encuentre protegida contra accesos no autorizados, los cuales pueden derivar en la alteración o robo de la información confidencial.
4. **Integridad.-** Significa que la información que se reciba sea precisa y este completa (su contenido es el necesario) para los fines que se consiguen

con su procesamiento, así como su validez, de acuerdo con los valores y las expectativas del negocio.

5. **Disponibilidad.-** Hace referencia a que la información necesaria para realizar cualquiera de las etapas del proceso administrativo este a mano cuando sea requerida por los procesos del negocio en cualquier momento.
6. **Apego a estándares**.- Significa que en el procesamiento de la información se deberán acatar leyes de uso general o reglamentos y acuerdos internos y contractuales a los cuales está sujeto el proceso de negocios.
7. **Confiabilidad.-** Significa que la información no haya sido alterada inapropiadamente.

Según (Yer, 2016) las medidas de seguridad en red, tratan de proteger los datos durante su transmisión, garantizar que los datos transmitidos sean auténticos la seguridad en computadoras y en redes implica cumplir con tres exigencias.

- **Secreto** implica que la información de un computador solo sea accesible para lectura de personas autorizadas.
- **Integridad** los recursos de un computador únicamente solo son modificadas por personas autorizadas
- **Disponibilidad** los recursos de un computador estén disponibles a personas autorizadas.

Tipos de ataques

Stalling hace la siguiente clasificación:

Ataque pasivos.

(DOUGLAS, 2015)También llamados escuchas, suponen el intento de un atacante de obtener información relativa de una información que está siendo transmitida, estos ataques son difíciles de detectar ya que no generan alteración a los datos.

Para tratar estos ataques hay que hacer énfasis en la prevención antes que en la detección una prevención pasiva bastante sutil es el análisis de tráfico.

Ataques activos

Supone la modificación de datos trasmitidos o la creación de transmisiones falsas se subdividen en 3 categorías.

- ✓ Repetición
- ✓ Modificación
- ✓ Denegación

Servicios de seguridad.

- ✓ Autenticación
- ✓ Confidencialidad
- ✓ Integridad

Según (Stallings, 2013) La fiabilidad distintos servicios de red pueden proporcionarse desde un circuito virtual fiable extremo a extremo hasta un servicio no fiable la operación de los rúter no debe depender de la suposición de fiabilidad de red.

Según (Bertolín, 2014) las redes que soportan información se están convirtiendo en elementos cada día más críticos para las actividades de trabajo

de cualquier organización y por ello necesitan estar protegido frente a posibles ataques.

Existe una relación directa entre el incremento y la importancia de factores estratégicos referente a los sistemas de información basados en red y el impacto potencial de las amenazas que lo pueden inutilizar o dañar de alguna forma, estas amenazas pueden dejar a la organización fuera de servicio rápidamente.

(ARIGANRLLO, 2014) La seguridad de los sistemas de información distribuidos se ha convertido en un factor crítico de primera magnitud y una obligación en el día a día de las actividades en todo tipo de organización.

(Aguilera, 2015) Según el modelo OSI (**O**pen **S**ystem **I**nterconnection), es un modelo conceptual que define los niveles o capas de hardware y software de las redes de comunicación de datos por donde circula la información.

No existen métodos ni protocolos establecidos para todos los modelos OSI, debido sobre todo a las diferentes topologías de red que existen y sobre todo a los sistemas que están implementados pero cada capa tiene sus propios protocolos.

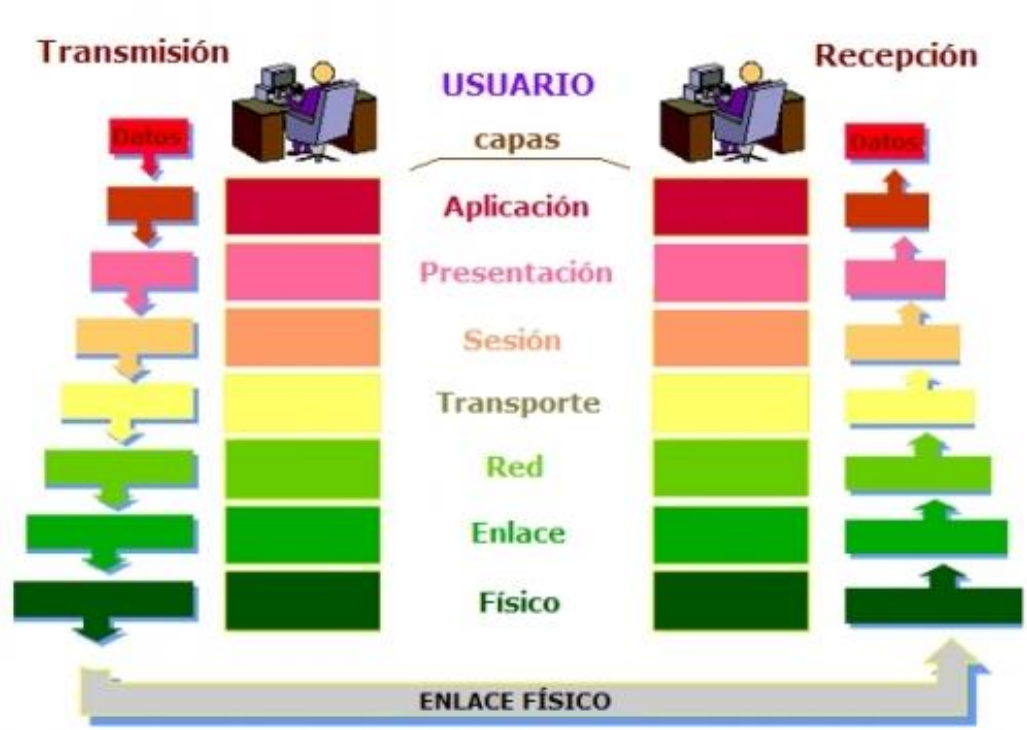

Imagen 2: Las 7 capas del modelo OSI
Fuente: http://www.itlearning.com

En la imagen # 2 se puede apreciar cada una de las capas del modelo OSI que se utilizan en una red de datos, cada uno de los niveles OSI tiene vulnerabilidades, se pueden aplicar medidas de protección para evitar la materialización de la amenaza, las vulnerabilidades y sistemas de seguridad sobres los que hay que profundizar en cada uno de ellos.

Según (Julian Veron Piquero, 2010) las principales normativas en seguridad son.

- ✓ Mecanismos de seguridad definidos en el estándar 801.11i
- ✓ Arquitecturas de seguridad descritas ISO/IEC 10181
- ✓ Estándares de claves y certificados de atributos X.509 describe los campos obligatorios y opcionales que deberían tener certificados.

La seguridad de red se consigue mediante el uso de criptografía el cual fragmenta sus algoritmos en dos grupos, Algoritmos de clave simétrica (clave secreta) cuando se utiliza la misma clave en ambos extremos de la comunicación.

Según (Soriano) cuando existen Deficiencias tecnológicas existen algunas deficiencias inherentes conocidas o desconocidas, o vulnerabilidades que pueden ser explotadas por un atacante suficientemente motivado.

(REDES Y HACKING, 2015) *El software para verificar la seguridad de red a utilizar son:*

Nmap

Nombrada como “herramienta de seguridad del año” por el Linux Journal, Network Mapper es una de las aplicaciones imprescindibles para administradores de sistemas, a la vez una de las fijas para hacking. Gratuita y de código abierto, funciona en Linux, Windows y Mac OS X. Se utiliza para realizar test de penetración, identifica los puertos abiertos o los servicios que se están ejecutando, ofrece la respuesta de computadoras a un ping. (REDES Y HACKING, 2015)

Esta herramienta, nos ayuda a encontrar peligros en cuanto a la seguridad de una red, es muy conocida a nivel mundial.

Nessus

Originalmente de código abierto, recientemente se ha convertido en software privativo pero sigue siendo gratuita para usuarios domésticos. Según los informes, es el escáner de vulnerabilidades más popular de Internet, utilizado por más de 75.000 empresas en todo el mundo. Nessus busca

puertos abiertos e intenta ataques con diversos exploits. Para usos de auditoría sobre una red propia se debe desactivar la opción “unsafe test” para no corromper el sistema. Funciona en Windows, Mac OS X y Linux, y puede ejecutarse en una computadora doméstica, en la nube o en un entorno híbrido. (REDES Y HACKING, 2015)

El presente estudio de caso cumple con la sub-líneas de investigación de la carrera de Ingeniería de Sistema en el cual es el modelo de **Trasmisión de Datos y Telecomunicaciones** en relación al **ESTUDIO DE LA SEGURIDAD DE LA RED DE DATOS DEL GAD FEBRES CORDERO para ser aplicada** en la Institución pública donde guarda información eficaz e importante para el desarrollo de La parroquia.

En el Gobierno Autónomo Descentralizado de Febres Cordero se utilizó el método inductivo, estudiando la vulnerabilidad de los datos almacenados y resguardados que posee la institución Pública.

En el desarrollo investigativo de la Seguridad de redes de Datos del GAD PARROQUIAL DE FEBRES CORDERO, se aplicó la técnica de observación directa de visualización de la seguridad de datos de la institución.

La seguridad de la Red de datos es muy importante en este medio dónde la integridad de la información es necesaria, esté presente las redes de área local, por eso es necesario la correcta configuración, para identificar si existe una falla o vulnerabilidad en el diseño.

Existen diferentes tipos de ataques a la red que no son virus, gusanos o troyanos, para esto es necesario tener categorizado los diferentes tipos de ataques.

GAD PARROQUIAL DE FEBRES CORDERO cuenta con el departamento talento humano, financiero, proyectos, información web.

La evaluación de riesgos se realizó con GFILanGuar software que proporciona una vista general de la red, también incluye los dispositivos USB Smartphone y tabletas conectadas, software que cuenta cada dispositivo, cualquier recurso compartido abierto, estado del hardware y contraseñas de baja seguridad en uso.

Imagen 3: software GFILanGuar
Fuente: Mauricio Campi

En la imagen # 3 se muestra de manera gráfica las debilidades en la red, la falta de actualizaciones nivel de seguridad, también genera una lista donde muestra los equipos conectados como los requerimientos, estados de firewall, credenciales, software antivirus en el medido se observa la baja seguridad en la red.

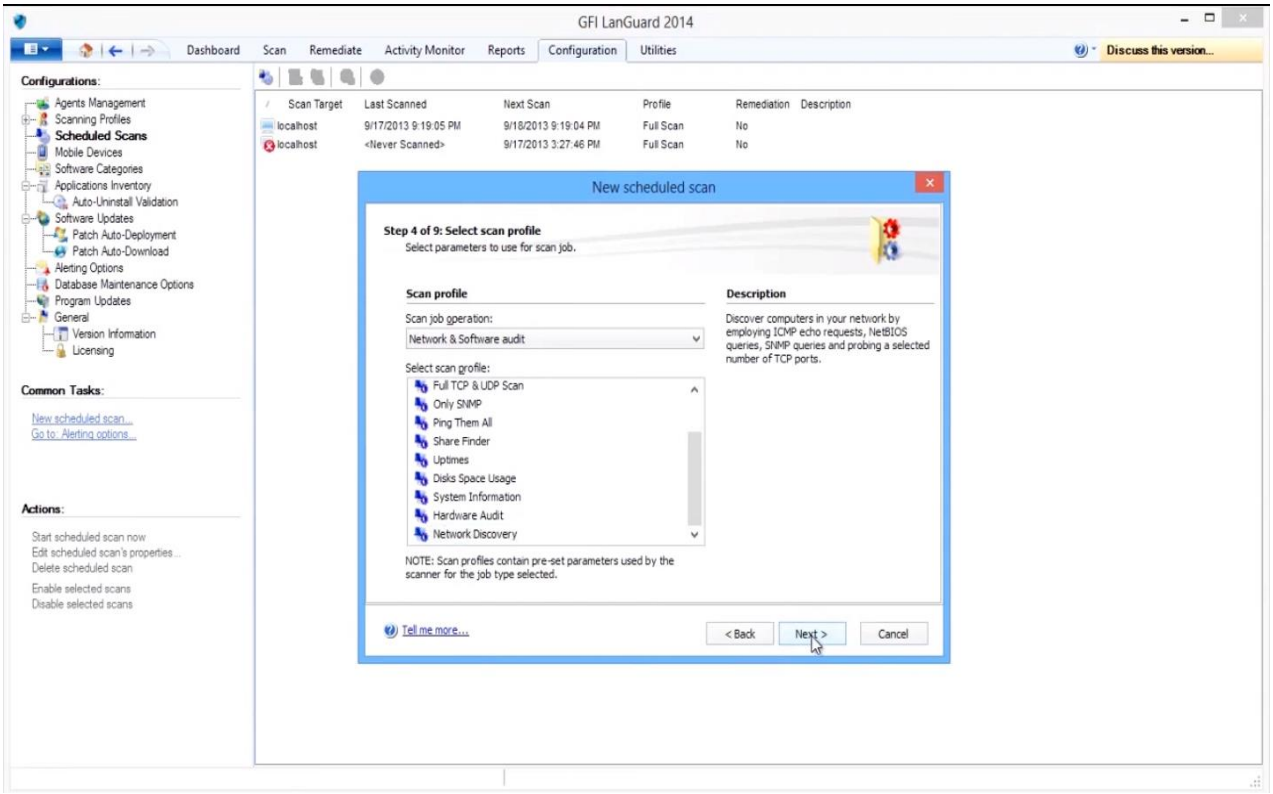

Imagen 4: Software GFILanGuar

Autor: Mauricio Campi

En la imagen # 4 se aprecia la manera de obtener información detallada de la configuración de los equipos de la red y también permite recuperar una lista de dispositivos

(SOFTWARE) Puede analizar fácilmente los resultados utilizando filtros e informes, lo que le permite asegurar proactivamente su red mediante el cierre

de puertos, eliminando usuarios o grupos que ya no se usan, o deshabilitando puntos de acceso inalámbricos.

GFILanGuard muestra información detallada sobre la configuración hardware de todos los equipos analizados en su red.

Recupera una lista de todos los dispositivos mediante la herramienta Administrador de Dispositivos de los sistemas operativos Windows®, incluyendo placa base, procesadores, memoria, dispositivos de almacenamiento, adaptadores de pantalla, y muchos más. Utilizando la vista histórica de red, ahora puede comprobar si se agregó o eliminó hardware desde el último análisis. (SOFTWARE)

Esto no significa que otros desarrollos o sistemas sean seguros. El hecho de que a nadie le importe lo suficiente un sistema como para hackearlo no significa necesariamente que sea seguro. Entre otras, se puede mencionar las siguientes deficiencias:

Deficiencias de la política de seguridad una deficiencia de la política de seguridad es una frase comodín para indicar que una política de seguridad de la empresa, (o tal vez, la falta de política), genera amenazas de seguridad en la red de forma inconsciente. Los siguientes ejemplos son algunas situaciones que pueden afectar negativamente al sistema informático de un negocio o empresa.

En el aporte del análisis se utilizaron diferentes tipos de software para los análisis en la seguridad en red como el Nmap, Nessus obteniendo mejores resultados de GFILandGuard, por lo que muestra un informe de manera gráfica a diferencia de otro software.

En este análisis se aplica la técnica de la entrevista, el cual se consultó a los encargados de las diferentes áreas del Gobierno Autónomo Descentralizado de Febres cordero, que tipos de percances o si acaso la institución habría sufrido algún tipo de ataques.

En el departamento de talento humano al investigar con el jefe del departamento supo manifestar que en los últimos 4 años por dos ocasiones habrían sufrido pérdida integral de información pero no había registro de que sucedió.

No obstante el encargado del departamento de información web supo manifestar que por varias ocasiones este servicio habría quedado inhabilitado.

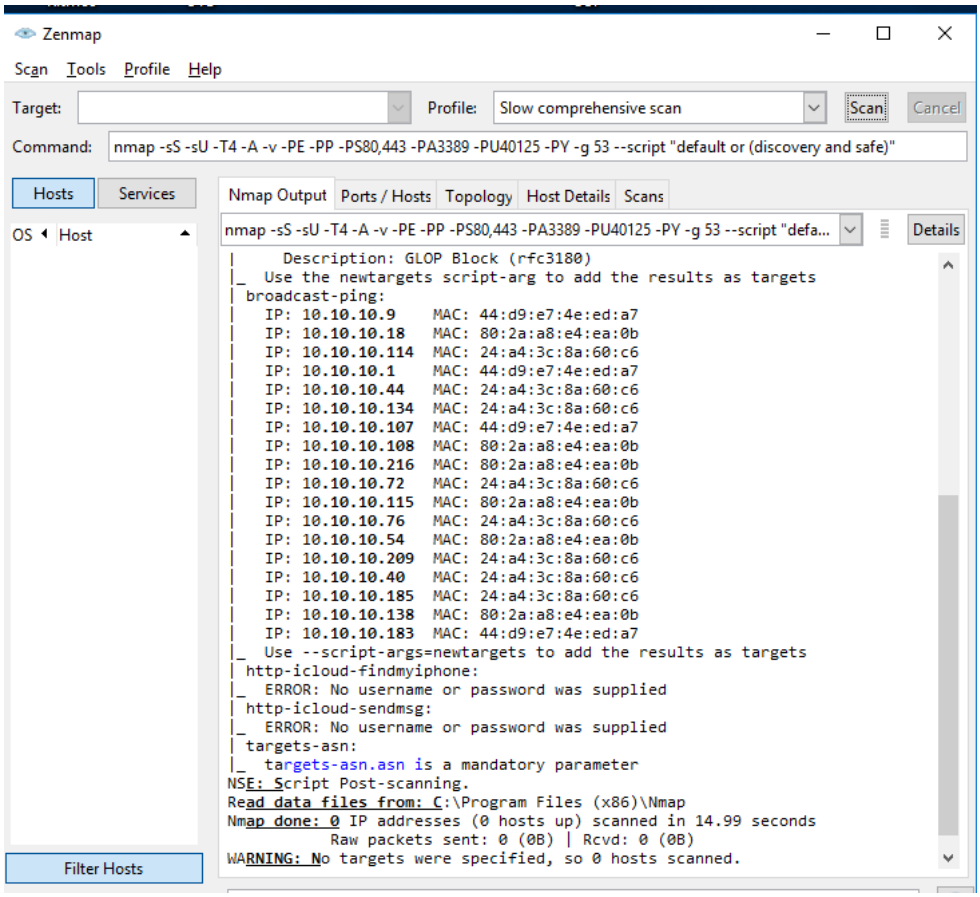

Imagen 5: software Zenmap
Fuente: Mauricio Campi

En la imagen # 5 se puede apreciar el análisis realizado por Nmap en el cual en uno de los nos muestra IP y direcciones MAC de cada dispositivo conectados en la red.

Conclusiones

Mediante la Investigación realizada se obtienen las siguientes conclusiones**:**

- Deficiencia tecnológica, no cuenta con software de seguridad, por tanto es vulnerable a afectaciones conocidas como desconocidas.

- Existe una deficiencia en políticas de seguridad de la empresa que genera amenaza de red de manera inconsciente.

- Existes ausencia de supervisión de seguridad

- No existe correo institucional, para brindar mejor seguridad a los usuarios.

- Deficiencia de configuración por contar con varios dispositivos de redes inalámbricas, con configuraciones básicas o configuraciones por defecto lo cual crea una puerta trasera de acceso.

Bibliografía

Aguilera, P. (2015). *REDES SEGURAS.* EDITEX.

ARIGANRLLO, E. (2014). REDES CISCO. BOGOTA: BOGOTA EDICIONES.

Bertolín, J. A. (2014). *SEGURIDAD DE LA INFORMACION DE REDES INFORMATICAS.* PARANINFO.

DOUGLAS, C. (2015). REDES DE COMPUTADORAS E INTERNET. MEXICO: PEARSON EDUCACIÓN.

Ernesto, A. (2014). *Redes CISCO.* Bogotá- Colombia: RA-MA.

Gómez, A. (2013). *Redes.*

GUZMAN, R. G. (enero de 2017). *http://repositorio.puce.edu.ec*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/13469/Disertacion-de-Grado-Ricardo-Aviles-Miguel-Silva.pdf?sequence=1&isAllowed=y

Julian Veron Piquero. (2010). *Prácticas de Redes.* LIBRIMUNDI.

LandGuard, G. (s.f.). Obtenido de https://www.gfihispana.com/products-and-solutions/network-security-solutions/gfi-languard: https://www.gfihispana.com/products-and-solutions/network-security-solutions/gfi-languard

pcexpertos.com. (s.f.).

REDES Y HACKING. (29 de 05 de 2015). Recuperado el 27 de 08 de 2018, de MUY COMPUTER: https://www.muycomputer.com/2015/05/29/herramientas-hacking-redes/

SOFTWARE, G. (s.f.). *Home Products and solutions GFI Security GFI LanGuard Características*. Recuperado el 08 de 2018, de GFILanGuarg: https://www.gfihispana.com/products-and-solutions/network-security-solutions/gfi-languard/specifications/network-and-software-auditing

Soriano, M. (s.f.). *IMPROVET*. Obtenido de SEGURIDAD EN REDES Y SEGURIDAD EN LA INFORMACION : http://Improvet.cvut.cz

Stallings, W. (2013). *Fundamentos de seguridad en redes.* Pearson Educación.

Torres, H. C. (3 de Octubre de 2013). *http://repositorio.ucsg.edu.ec.* Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/1399/1/T-UCSG-PRE-TEC-ITEL-13.pdf

Urbina, G. B. (2016). *Introduccion a la Seguridad Informatica.*

Yer, A. C. (2016). *ESTUDIO CIENTIFICO DE LAS REDES.* VISION LIBROS.