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

Tema:

Análisis de amenazas, vulnerabilidades y problemas de interconexión en el sistema de internet de la empresa Monvision s.a. de la ciudad de Montalvo.

Egresado:

Xavier Patricio Paredes Avila.

Tutor:

Ing. Raúl Ramos Morocho.

Babahoyo - Los Ríos

2019 – 2020

Introducción

La presente investigación tiene como finalidad determinar cuáles son las amenazas, vulnerabilidades y problemas de interconexión de la empresa proveedora de internet Monvision S.A. por el motivo que ha presentado algunas anomalías con el servicio de internet contratado por los usuarios, los cuales la empresa deberá corregir para evitar pérdida de clientes e ingresos en el futuro y ofrecer un mejor servicio.

Los servicios proveedores de internet se han convertido en uno de los mayores fuentes de generar ingresos y empleos de la última década, ya que la mayoría de personas y empresas usan el internet en su diario labor de manera directa e indirecta, poniendo como referencia un artículo publicado por el diario El Comercio en el cual indica que "el 82% de la pymes usan internet en su vida laboral" (Orozco & Quiroz, 2015), convirtiéndose en parte fundamental de la vida natural, académica y comercial de las personas.

En la actualidad MONVISION S.A. se ha convertido en uno de los mayores proveedores de internet del cantón Montalvo con aproximadamente 980 usuarios que usan dicho servicio, siendo la primera empresa en ofrecer el servicio de distribución de internet a través de fibra óptica en el cantón Montalvo.

Gracias a la gran velocidad de descarga de datos que provee Monvision S.A. tiene gran demanda en los usuarios, los mismos que usan la red para sus vidas natural y laboral conectando sus dispositivos personales a la red los cuales contienen tienen información de interés, considerado esta como el activo más importante de cada empresa, y dicho activo debe estar protegido al conectarse a la red, para no ser robado, alterado o eliminado por personas con un fin malicioso.

El siguiente estudio de caso está enfocado en realizar un análisis de cuáles son las posibles amenazas, vulnerabilidades o problemas de interconexión en el sistema de internet que provee la empresa Monvision S.A. para ofrecer una mayor seguridad sobre los datos de cada uno de los usuarios que dispone dicha empresa.

El estudio de caso se realizó siguiendo la sub-línea que se ubica en los procesos de trasmisión de datos y telecomunicaciones, se utilizó la metodología inductiva la cual conlleva razonar a partir de una serie de observaciones para determinar cuáles serias los posibles amenazas, vulnerabilidades y problemas de interconexión de la empresa Monvision S.A.

Primero se realizó una muestra estadística a los usuarios que tiene la empresa en la actualidad para posteriormente realizar una encuesta a dicha muestra y ver cuales habían sido los problemas que tenía los usuarios beneficiaros de esa red.

Para poder realizar el análisis de amenazas y vulnerabilidades se utilizó el Software Nessus el cual realiza un escaneo en la red desde un usuario cliente para mostrar posteriormente todos los puertos que son vulnerables para cualquier ataque que represente una amenaza.

Para revisar los problemas de interconexión se realizó un testeo de velocidad de bps (bytes second o bytes por segundo) para poder observar cual era la velocidad de descarga que tenía la red, para lo cual se usó Fast.com y Speedtest.net medidores de velocidad de descarga gratuitos.

Desarrollo

En la actualidad casi todas las empresas públicas o privadas, así como las personas naturales usan de una manera diaria, las herramientas tecnológicas de información como medio principal para logras sus fines laborales y personales en su vida diaria. De la misma forma todos los dispositivos son propensos a amenazas y vulnerabilidades que tienen que ver con los medios informáticos.

La información, considerada como uno de los activos más importantes de cada empresa o persona, es la más propensa a sufrir robos, perdidas o alteraciones, por lo cual la seguridad informática debe estar legada a proteger la propiedad intelectual de cada entidad o usuario.

Las amenazas informáticas son el riesgo que corren todos los usuarios que se conectan diariamente a la red, ya que el vandalismo computacional se manifiesta en muchas formas, con el fin de dañar o destruir. Existen programas como Troyanos (nombre que hace referencia al caballo de Troya relatada en la Odisea de Homero) que se disfrazan de algo inofensivo que se activan al momento que el usuario los abre o ejecuta.

Las vulnerabilidades son fallos de seguridad que causan una debilidad en los sistemas o dispositivos tecnológicos que son aprovechados por los delincuentes, se consideran ellos fallos para corregirlos por los desarrollares en la siguiente versión o actualización que se lanza al sistema operativo. Estos pueden ocasionar gran perjuicio a las entidades y violar la integridad de la información.

> *"Los avances de las telecomunicaciones y en los softwares de los equipos han aumentado las amenazas y debilidades que vulneran los sistemas que pueden ser interconectados en diferentes puntos, siendo así el potencial para acceder no autorizado, como fraude o abuso no se limita a un solo punto, sino que puede*

> *ocasionar áreas de acceso a la red, lo que diseña nuevas oportunidades y áreas para ingresar a los sistemas."* (Cano Alaba, 2017)

Existen también los gusanos que programas que se mueven dentro de la red de dispositivo en dispositivo dañando el sistema y enviando la preciada información a sus creadores.

Las empresas encargadas de proveer internet a otras empresas y familias, deben considerar cada uno de los factores que pueden ser llamadas amenazas, vulnerabilidades o problemas de interconexión, los cuales se presenten a los usuarios.

> Según (Ramos Morocho & Vega Villacís, 2017) *"Hoy en día, teniendo en cuenta el avanzado ritmo de la tecnología, las empresas e instituciones sean públicas o privadas adoptan medidas de protección y seguridad para preservar su bien más preciado, la información, ya que del mismo modo se han hecho presentes los ataques informáticos e infiltraciones no autorizadas de personal ajeno o mal intencionado para cometer acciones ilícitas o sacar ventaja competitiva."*

TIPOS DE AMENAZAS.

Al hablar de las amenazas de los sistemas de internet que ofrece un proveedor de internet las podemos clasificar en Factores humanos, Factores naturales, Fallos en procesamiento de información y descarga de datos, y sucesos maliciosos.

FACTORES HUMANOS

Se deben a fallos accidentales o errores que comenten las personas en sus actividades laborables o personales, como dejar la sesión abierta su usuario de la oficina en la cual otras personas puedan modificar información o desactivar servicios, aumentar o disminuir el ancho de banda permitido para cada cliente, etc.

Otro de los problemas más comunes suele ser la mala manipulación de los routers por los usuarios, ocasionando que estos accedan a los mismos y modifiquen las IP asignadas generando conflictos en la red. *"Cuando se trata de una falla de colgar del vehículo, el cable de fibra óptica en el punto defectuoso debe probarse en dos direcciones primero para confirmar la cantidad de cables ópticos bloqueados y luego tratarlo de manera específica."* (Softel, 2019)

FACTORES NATURALES

Desastres naturales como lluvias, tormentas, tempestades, arboles, derrumbes, etc., los cuales dañen los equipos de conexión de internet, los postes pueden desplomarse y arrancarse las fibras que se encuentran conectadas, la caída de rayos puede ocasionar que los switchs repartidores de señal sufran cortocircuitos, etc.

> *"Si la temperatura es demasiado baja, el agua en la caja de empalme se congelará, la cubierta del cable óptico se encogerá longitudinalmente y la micro flexión causada por la presión sobre la fibra óptica aumentará la atenuación o la interrupción. La fibra óptica. Si la temperatura es demasiado alta, dañará fácilmente la cubierta del cable óptico y otros materiales de protección y afectará las características de la fibra óptica."* (Softel, 2019)

FALLOS EN PROCESAMIENTO DE INFORMACIÓN Y DESCARGA DE DATOS

El exceso de tráfico de datos puede ocasionar una congestión al momento de la subida y bajada de datos, esto suele suceder cuando los proveedores tienen más clientes de los que puede soportar la red, esto puede ocasionar malestar entre los usuarios ya que bajaría el ancho de banda contratado, esto generalmente ocurre en las denominadas horas picos del internet, cuando todos los usuarios están en casa.

SUCESOS MALICIOSOS

Son actos vandálicos ocasionados por terceros, con la finalidad de realizar daños o difamación de la empresa con el fin de desprestigiar a la misma, congestionarla o robar datos, evitando que los usuarios tengan una navegación apropiada, generando malestar en los últimos.

ATAQUES INFORMATICOS

Los ataques son uno de los delitos con más renombre en la actualidad, según la encuesta de seguridad realizada cada año por el FBI, los virus o ataques informáticos son la fuente principal que genera perdida financiera y de datos.

El viceministro del Ecuador revelo que el país en el mes de abril del 2019 recibió más de 40 millones de ataques cibernéticos, lo cuales fueron vinculados a Estados Unidos y Reino Unido, "*Los ataques provienen de Estados Unidos, Reino Unido e incluso de Ecuador; entre las entidades atacadas están Cancillería de Ecuador, Presidencia de la República, Banco Central del Ecuador, ministerios y GAD´s.*" según (Rivadenieria , 2019), los mismos que fueron efectuados después que Ecuador decidido retírale el asilo diplomático a Julian Assange, fundador de WikiLeaks.

Seguridad de red y sus vulnerabilidades

Al hablar de seguridad de red, en primer lugar, debemos conocer sobre que vamos a proteger: La información. De tal manera que definimos el definimos el dato como la unidad mínima de información siendo la misma. Así mismo definimos la información como un conjunto de datos que tienen un significado específico.

Los sistemas de seguridad informáticos deberán estar lo suficientemente sofisticados o preparados para poder compensar y garantizar la disponibilidad, confidencialidad e integridad de información ante cualquier ataque. (Solórzano Cadena & Rezabala Triviño, 2016)

Los tipos de información que existen son: públicas y privadas.

Información pública es aquella que está al alcance de todas las personas en particular y que es un derecho que garantiza el estado según Ley Orgánica de Transparencia y Acceso a La Información Pública en su registro aprobado por el congreso en él 2004 (Lexis, 2018), mientras que la información privada es limitada solo a un grupo de personas determinadas que trabajan con la misma.

Se utilizan diversos métodos para quebrar

Se utilizan diversos métodos o técnicas para quebrar o vulnerar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del software o sistema para poder acceder en él. El trabajo de los administradores o ingenieros no difiere mucho de esto. En lo que sí se diferencian, es en los objetivos: *"un intruso penetra en las redes de computadoras para distintos fines (investigación, daño, robo, etc.) mientras que un administrador lo hace para poder mejorar los sistemas de seguridad."* (Mancheno Torres & Robles Coronel, 2016)

Análisis de amenazas, vulnerabilidades y problemas de interconexión en el sistema de internet de la empresa Monvision s.a. de la ciudad de Montalvo.

Siendo Monvision S.A. una de las principales empresas proveedoras de internet del cantón Montalvo, está encargada de ofrecer a todos los usuarios una seguridad al momento de navegar dentro de la red, y realizar cada una de las tareas y transacciones de manera segura, tranquila y rápida, de manera que no tenga problemas al momento de navegar por la web cumpliendo las expectativas demandadas por los clientes.

Para realizar el siguiente estudio de caso se procedió a realizar una pequeña muestra a los clientes que son beneficiaros del servicio de internet, se procedió a realizar una encuesta a 63

personas al azar, en un día común en las oficinas de recaudación de Monvision S.A. la cual acepto con el fin de ofrecer un mejor servicio a sus clientes.

Al realizar la encuesta se pudo determinar que cerca del 70% de los clientes tuvieron algún problema con la navegación de internet a través de la red de Monvision S.A. de las cuales un 32% de los usuarios comenta que se debieron por fallos en los routers los mismos que fueron reconfigurados por los técnicos de la empresa, o cambiados en algunos de los casos.

Amenazas y vulnerabilidades de Monvision S.A.

Podemos definir como amenaza a toda o mecanismo capaz contra la seguridad de información.

Las amenazas son consecuencias que surgen debido a la existencia de vulnerabilidades, de manera que podemos decir que una amenaza surge a partir del aprovechamiento de vulnerabilidades, las cuales comprometan dependiente o independientemente a la seguridad de la información.

Una de las vulnerabilidades que tiene la empresa es el fácil acceso que tiene el usuario para ingresar a las configuraciones del router ya que tienen el usuario y la contraseña por defecto (usuario: admin, password: admin), en la cual los usuarios muchas veces modifican las configuraciones establecidas por los técnicos perdiendo así conectividad a la red.

Figura 1. *Acceso al router, Usuario: admin, Password: admin.*

Una vez que el usuario ha accedido al router le resulta muy fácil modificar cada uno de los valores que el técnico dejo previamente configurado para su correcto funcionamiento.

Figura 2: *Configuraciones del router después de acceder al mismo.*

Se realizó un escaneo en la red mediante un usuario cliente para poder analizar cuáles sean sus vulnerabilidades de la red, para eso usamos:

Nessus como software el cual permite ver cuáles son los puertos vulnerables a través de un escaneo sobre la red con el sistema operativo Windows.

Después de realizar les escaneo se determinó que posee once puertos vulnerables, los cuales pueden ser aprovechados por hackers para realizar cyber-ataques a la red con el propósito de vulnerarla y provocar amenazas a la misma.

Se pudo detectar seis puertos los cuales son.

139/tcp/smb .- Usados para el "*intercambio de archivos y uso compartido de impresoras en la red. Lo cual es usado por terceros para acceder a red y estos servicios."* (Cooper, 2017). Velase figura 6 del Anexo III.

18182/tcp.- Es un puerto bidireccional esto "*garantiza la entrada de paquetes en el mismo orden en que fueron enviados, la verificación y corrección de errores no es necesaria o cumplida en la aplicación, para evitar gastos en la interface de red."* (Kantor, 2017) Velase figura 7 del Anexo III.

23/tcp.- Es uno de los protocolos más antiguos que existe, además de ser el "*programa más popular para realizar un acceso remoto a las maquinas Unix."* (SG Security Scan, 2018). Tiene muchas vulnerabilidades de seguridad. Velase figura 7 del Anexo III.

445/tcp/cifs.- Cifs, sucesor de SMB(Protocolo del bloque de mensaje), uno de los principales protocolos usados por Windows para compartir archivos, "*su sistema de almacenamiento recibe y remite datos a través de este puerto, usado solo sobre IPv6, lo cual requiere solo servicios de archivos de Windows para cumplir su función."* (Castro, 2016) Velase figura 8 del Anexo III.

53/tcp/dns. - DNS(Servicio de nombres de Dominio) Es usado para la resolución de nombres de dominio, *"los ataques generalmente son usando sus vulnerabilidades, penetrando con algunos troyanos o gusanos (ADM, MscanWorm, li0n, entre otros)."* (Wiley & Inc, 2018) Velase figura 8 del Anexo III.

80/tcp. - "*Es el protocolo de transferencia de hipertexto HTTP, usado por Word Wide Web, FaceTime, iCloud, etc.".* (Apple, 2016) básicamente por casi todos los servidores web para responder a la petición hecha por un cliente en específico, este no guarda ninguna información sobre conexiones anteriores. Velase figura 8 del Anexo III.

También con el sistema operativo Kali Linux ser realizo un análisis con la herramienta nmap, para realizar un escaneo a la red a través del router el cual mostro cuatro puertos abiertos y uno haciendo la función de un cortafuego.

21/tcp. - El protocolo de transferencia de ficheros el cual se usa para conexiones con servidores FTP. (Espinosa, 2019) Véase figura 10 Anexo III.

Problema de interconexión

Los principales problemas que ocasionaban dichos routers era el colapso en la red al conectar muchos dispositivos en la red o después de permanecer encendido por un tiempo extendido, por lo cual se procedía a reiniciar el mismo procedía a solucionar dichos errores de manera temporal, dichos routers fueron remplazados por unos de mejor calidad, solucionando uno de los problemas de interconexión más común que presentaba la empresa.

Figura 3: *Router que usaba la empresa Monvision S.A. en las primeras instalaciones.*

Para solucionar algunos problemas de conexión con la red, y colapsos dentro de las mismas se remplazaron los routers por unos de mejor calidad.

Figura 4: *Router que usados actualmente por la empresa Monvision S.A*

Otros de los problemas de interconexión que se han presentado en la empresa se debió a factores externos o naturales, como daños en los puntos de conexión por sobrecargas, caídas de rayos, etc., así mismo por cables fibras óptica arrancados por la caída de árboles, vehículos voluminosos, animales como zarigüeyas o perezosos, o ineptitud humana.

La congestión en la red en un rango determinado del día resulto ser uno de los problemas con un rango de 57% entre los usuarios, los cuales declaraban que en horas de la noche tenían perdía de datos en la velocidad de descarga. Véase el Anexo II.

Para solucionar aquel problema la empresa aumento el ancho de banda de 540mbs a 950mbs además de hacerse acreedores de servidores privados gratuitos de Google y YouTube con los cuales se reduce el consumo de megas por cliente ofreciendo una mejor experiencia en la navegación por cada usuario. Véase el Anexo III Figura 4,5,6

Tabla comparativa de especificaciones técnicas de los router

	Router FIBERARK CA196 (Antes)	**Router FIBERARK FE702 (Después)**
Puertos	1 FIBERPORT, 4 LAN, 1 Salida coaxial, 1 Alimentación	1 FIBERPORT, 1 LAN, 1 alimentación
Indicadores Led	Alimentación, DMZ, WLAN, Lan (1, 2, 3, 4), Internet, CATV	Alimentacion, Internet, Los, Lan, Wifi
Botones	Reset, Power	Reset, Power
Temperatura de funcionamiento	0° a 40°	0° a 40°
Temperatura de Almacenamiento	-10° a 53 °	-20 a 72°
Tasa de enlace máxima	100Mbps	300Mbps
Compatibilidad	Windows, Linux, Mac	Windows, Linux, Mac

Esquema de la Red

Figura 5: *Esquema de la red.*

Estándares de la red.

En la actualidad la red y el cableado no se rige por una estandarización de red, o cableado estructurado normalizado de manera oficial, debido a al desconocimiento de los mismos, cabe destacar que, si cuenta con un cableado estructurado en la red, de esta manera tiene organizado y resulta más fácil corregir una falla por sectores gracias a la correcta señalética que cuenta la red. Véase anexo 4, figura 5.

Ficha de Observación

<table>
<tr><td rowspan="2">Ficha de observación</td><td>Caso de estudio: Análisis de amenazas, vulnerabilidades y problemas de interconexión en el sistema de internet de la empresa Monvision s.a. de la ciudad de Montalvo.</td></tr>
<tr><td>Responsable: Paredes Avila Xavier Patricio</td></tr>
<tr><td>Fecha: 2020, enero 16.

Hora: 14:00.

Lugar: Departamento de distribución de internet de la empresa Monvision S.A.</td><td>Observaciones.
Se realizo un análisis con la herramienta Nessus en el sistema operativo de Windows y nmap en el sistema operativo Kali Linux, con la cual su puedo observar siete puertos trabajando dentro de la red a través del router de los cuales seis puertos se encontraban abiertos haciendo vulnerable a la red ya que por medio de ellas accederían para realizar un ataque.

El centro de distribución no tiene amenazas de factores naturales que puedan ocasionar un daño a la infraestructura ya que no hay la existencia de árboles cercas las cuales puedan ocasionar daños al cableado principal de la red Véase figura 11 Anexo IV.

La infraestructura externa muestra un deterioro, la cual requiere un mantenimiento, mientras que el interior si aplica un cableado estructurado teniendo de manera organizada lo cual permite corregir un error de conexión de manera más fácil cuando este se presente. Véase figura 12 Anexo IV.</td></tr>
</table>

BIBLIOGRAFÍA

Apple. (2016). *Apple*. Obtenido de Puertos TCP y UDP que se usan en los productos de software de Apple: https://support.apple.com/es-co/HT202944

Borghello, C. (2005). *Linux máxima Seguridad.*

Cano Alaba, J. M. (2017). *Repositorio DigitalUniversidad Tecnica de Babahoyo Repositorio Digital*. Obtenido de http://dspace.utb.edu.ec/handle/49000/2428

Castro, R. (2016). *Uso de puerto IP en un sistema de almacenamiento*. Obtenido de NetApp: https://library.netapp.com/ecmdocs/ECMP1114171/html/GUID-45640E38-88B6-4AA7-9D36-90C1076E1A76.html

Cooper, S. B. (2017). *Techlandia*. Obtenido de ¿Qué es el puerto 139?: https://techlandia.com/puerto-139-info_235022/

Espinosa, O. (27 de Octubre de 2019). *Redes Zone*. Obtenido de https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

Kantor, A. (abril de 2017). *Iana*. Obtenido de https://www.iana.org/

Lexis. (2018). *Superintendencia de Economia Popular y Solidaria*. Obtenido de https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Mancheno Torres, H. C., & Robles Coronel, I. L. (2016). *Repositorio Digital Universidad Católica de Santiago de Guayaquil.* Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/1399

Orozco, M., & Quiroz, G. (19 de julio de 2015). *El Comercio*. Obtenido de https://www.elcomercio.com/actualidad/pymes-internet-ecuador-tecnologia-empresas.html

Ramos Morocho, R. A., & Vega Villacís, G. (2017). Vulnerabilidades y amanezas a los servicios web de la intranet de la Universidad Técnica de Babahoyo. En *3ciencias* (págs. 53 - 66).

Rivadenieria , G. (15 de abril de 2019). Ecuador ha recibido 40 millones de ataques cibernéticos, revela viceministro de Telecomunicaciones. *El Universo*.

SG Security Scan. (2018). Obtenido de https://www.speedguide.net/scan.php

Softel. (07 de diciembre de 2019). Obtenido de http://m.softelftth.com/

Solórzano Cadena, L., & Rezabala Triviño, J. (2016). *Estudio sobre el estado del arte de la seguridad informática en el Ecuador y sus necesidades reales.* Obtenido de Repositorio Espol: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/24298

Wiley, J., & Inc, S. (2018). *Inflobox Next level networking*. Obtenido de www.infoblox.com/dns-security-resource-center/dns-security-faq/is-dns-tcp-or-udp-port-53

CONCLUSIONES

Después de realizar el estudio de caso sobre análisis de amenazas, vulnerabilidades y problemas de interconexión en el sistema de internet de la empresa Monvision s.a. de la ciudad de Montalvo, se determinó que la red de Monvision S.A. tenía vulnerabilidades en seis puertos los cuales podrían ser usados por hackers o ladrones informáticos con fines ilícitos como de acceder a la red y robrar información de los usuarios que contratan dicho servicio.

Los fallos de interconexión que sufrían algunos usuarios se debían a los de mala calidad que uso la empresa en las primeras instalaciones los cuales sufrían colapsos al estar encendidos por mucho tiempo y se tenían que reiniciar continuamente causando malestar en algunos usuarios, los cuales fueron retirados y posteriormente cambiados por unos de mejor calidad.

Además, los router tenían un fácil acceso a sus configuraciones de parte de los usuarios ya que tenían sus usuarios y contraseñas de acceso por default, los cuales eran modificados por los clientes con poco conocimiento, perdiendo la conexión con la red.

Resumen

La presente investigación tiene como propósito determinar cuáles son las amenazas, vulnerabilidades y problemas de interconexión de la empresa proveedora de internet Monvision S.A. por el motivo que ha presentado algunas anomalías con el servicio de internet contratado por los beneficiarios, los cuales la empresa deberá corregir para evitar pérdida de clientes e ingresos en el futuro y ofrecer un mejor servicio.

Gracias a la gran velocidad de descarga de datos que provee Monvision S.A. tiene gran demanda en los usuarios, los cuales usan la red para enviar datos desde cada uno de sus a través de la red.

Primero se realizó una muestra estadística a los usuarios que tiene la empresa en la actualidad para posteriormente realizar una encuesta a dicha muestra y ver cuales habían sido los problemas que tenía los usuarios beneficiaros de esa red.

Para poder realizar el análisis de amenazas y vulnerabilidades se utilizó el Software Nessus el cual realiza un escaneo en la red desde un usuario cliente para mostrar posteriormente todos los puertos que son vulnerables para cualquier ataque que represente una amenaza.

Para revisar los problemas de interconexión se realizó un testeo de velocidad de bps (bytes second o bytes por segundo) para poder observar cual era la velocidad de descarga que tenía la red, para lo cual se usó Fast.com y Speedtest.net medidores de velocidad de descarga gratuitos.

Palabras claves

Análisis, Vulnerabilidades, Amenazas, Problema de interconexión, Puertos abiertos.

ANEXOS I

Calcular la muestra

La empresa consta actualmente 980 clientes los cuales tienen contratado el servicio de televisión por cable e internet a través de fibra óptica, para lo cual se ha procedido a realizar una pequeña muestra para poder efectuar una encuesta a los clientes de dicha empresa, la cual se expresa a continuación.

- N= 980 (Población)
- e=10% (Margen de error)
- z= 90% = 1.65 (Nivel de confianza)
- p= 0.5% (Probabilidad a favor)
- q= 0.5% (Probabilidad en contra)

$$\boldsymbol{n = \frac{z^2 * p * q * N}{e^2(N-1) + z^2 * p * q}}$$

$$\boldsymbol{n = \frac{1.65^2 * 0.5 * 0.5 * 980}{0.1^2(980-1) + 1.65^2 * 0.5 * 0.5}}$$

$$\boldsymbol{n = \frac{667.0125}{10.470625}}$$

$$\boldsymbol{n = 63.070}$$

Un total de 63 personas de encuestadas fueron un numero promedio ideal para poder llevar a cabo el siguiente estudio.

Anexo II

Cuestionario de las preguntas realizadas en la encuesta.

1. **¿Ha tenido problemas con la navegación de internet?**

   La encueta realizada, mostro que el en los primeros meses de contratación de servicio el 32% de personas tuvieron problemas de interconexión las primeras semanas de contratación del servicio, las cuales fueron corregidas después por los técnicos de la empresa.

2. **¿Cuáles han sido los problemas que ha presentado la conexión?**

   Los clientes comentan que el principal problema de conexión que han presentado es lentitud al momento de navegar después de algunos días de uso continuo, lo cual solucionan reiniciando los routers.

3. **¿Cuánto ha sido el tiempo de respuesta que tiene la empresa en resolver un problema?**

   Los clientes comentan que el tiempo en resolver un problema dentro de la red ha sido en la mayoría de los casos de pronta respuesta. Esto se debe a que la empresa tiene técnicos encargados de solucionar todos los problemas dentro de las casas u oficinas en un rango de 24 horas como máximo, y por daños causados por factores externos (equipos dañados por cortocircuitos o rayos, fibras arrancadas, etc.) con un periodo máximo de 72 horas.

4. **¿Ha sufrido usted una pérdida o robo de información al momento de navegar por la web usando el internet que provee Monvisión?**

   Las personas que participaron en la encuesta comentan que nunca han sufrido robo o perdida de datos en todo el lapso de tiempo que han contratado el servicio.

5. **¿Ha tenido problemas de infección maliciosas de virus informáticos?**

Las personas comentan que si has tenido problemas de infecciones maliciosas o virus informáticos en sus equipos de cómputo dentro de la web.

6. **¿Con que dispositivo se conecta usted usualmente a la red?**

   El 61% de las personas usan el internet par navegar por un ordenador, televisor o smartphone, mientras que el 24% solo usan para navegar a través de smartphones o tablets.

7. **¿Cuáles son los sitios web que navega frecuentemente?**

   El 73% de las personas que navegan por paginas universitarias o para realizar trabajos, mientras que el 27% lo usa para navegar por las redes sociales o sitios que ofrecen películas o música mediante streaming.

8. **¿Puede acceder de manera fácil a las configuraciones del routers?**

   El 79% de los clientes declararon que desconocen cómo acceder a las configuraciones del router y modificar las mismas, de la misma encuesta se dedujo que 17% de las pueden acceder y modificar las configuraciones del router, y el 4% cuenta haberse quedado sin internet después de modificar dichas configuraciones.

9. **¿Cuáles son las horas en las que sufre colapso en la red?**

   El 57% de los usuarios comentan que tienen problemas con la navegación en las horas de la noche poniendo como rango de las 19:00 hasta las 23:00, mientras que el 16% dicen que no tienen problemas ni colapsos en la red.

10. **¿Ha notado comportamiento inusual en la forma de navegación de los niños?**

    El 67% de las personas encuestadas comentan que los niños solo navegan en redes sociales y juegos online, mientras que el 33% no le prestan interés a los sitios en los cuales sus hijos navegan.

Anexo III

Capturas de pantalla de la de descarga que ofrece la empresa a sus clientes:

1. Antes de aumentar el ancho de banda

Figura 6: *Test de velocidad Fast, usado con routers de mala calidad.*

Como podemos apreciar la velocidad sufría caídas de la capacidad de bps de descarga, lo cual se debía al poco ancho de banda de la empresa y la deficiencia causada por los routers de mala calidad, los cuales necesitaban un reinicio continuo para su funcionamiento.

2. Después de aumentar el ancho de banda

    a. Test de velocidad con Fast, servidor de Netflix

Figura 7: *Test de velocidad Fast con router nuevos.*

b. Test de velocidad con SpeedTest, servidor Claro.

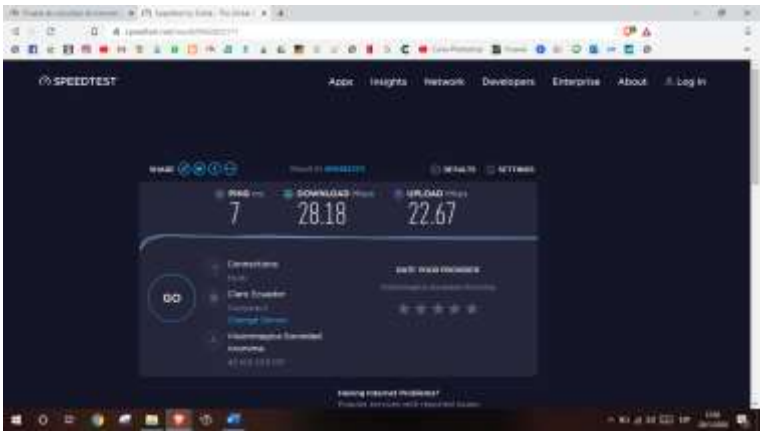

Figura 8: *Test de velocidad SpeedTest con router nuevos.*

Escaneo realizado a la red de Monvision S.A. con el software Nessus

Después de realizar el escaneo se mostró que hay 19 vulnerabilidades en la red local, de los cuales ocho pertenecen a la puerta de enlace con la red (Router). Los cuales se muestran a continuación.

Figura 9: *Análisis de vulnerabilidad en el puerto 139/tcp/smb.*

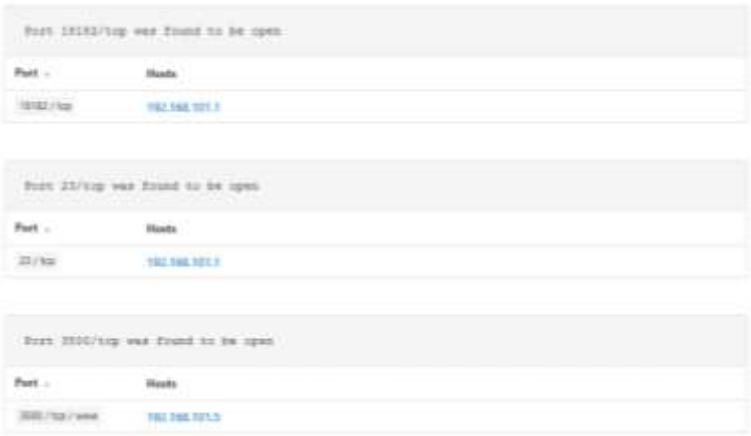

Figura 10: *Análisis de vulnerabilidad en el puerto 18182/tcp y 23/tcp*.

Figura 11: *Análisis de vulnerabilidad en el puerto 445/tcp/cifs, 53/tcp y 80/tcp.*

Se muestra a continuación el análisis completo realizado por Nessus el cual encontró 19 vulnerabilidades de las cuales seis se presentaron sobre la red y 13 sobre equipo que realizo el escaneo.

Figura 12: *Análisis de vulnerabilidad detallado por la herramienta Nessus.*

Se muestra el análisis realizado con el sistema operativo usando la herramienta nmap, el cual mostro cuatro puertos abiertos en tcp y uno que activa el filtro de paquetes, por lo general el firewall.

Figura 13: *Análisis de vulnerabilidad detallado por la herramienta nmap en el sistema operativo Kali Linux.*

Anexo IV

Fotos del centro de distribución de internet de la empresa Monvision S.A.

Figura 14: *Centro de distribución de internet de la empresa Monvision, parte externa.*

Figura 15: *Centro de distribución de internet de la empresa Monvision, parte interna.*