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 INTERCONECTIVIDAD Y SEGURIDAD DE DATOS EN LA F.A.F.I

EGRESADO:

KEVIN ALEJANDRO FONSECA BARRAGÁN

TUTORA:

LCDA. GLADYS PATRICIA GUEVARA ALBÁN, MIE.

AÑO 2018

I. INTRODUCCION

En la actualidad la seguridad de datos y la interconectividad van de la mano, se han creado procedimientos y tecnologías de seguridad disponibles para salvaguardar la integridad de los datos, pero no se puede afirmar que estén completamente a salvo de los intrusos.

La seguridad de datos se enfoca en la protección de la infraestructura y de toda la información incluida en un ordenador.

Se puede decir que las principales características de la seguridad de datos son:

- La integridad de los datos.
- La Confidencialidad.
- Disponibilidad.

Jean François Carpentier dice que la protección de datos es esencial, sea cual sea su tamaño, a partir del momento en que toda la información importante se almacena en la infraestructura de su red. (Carpentier, 2016)

En términos general lo que es la interconectividad es la comunicación de dos o más redes, que utilizando la red al máximo podemos compartir recursos, acceso a las bases de datos compartidas.

La facultad se encuentra conformada por seis carreras que son Ingeniería Comercial, CPA, Ingeniería en Sistemas, Ingeniería en Sistemas de Información, Contabilidad y Auditoría, Comercio, donde al pasar los tiempos se implementó una plataforma académica con el fin de mantener de forma segura y factible el acceso los datos, agilizando así procesos académicos los cuales en tiempos pasados no impartían confianza.

La plataforma tecnológica ha sido de gran ayuda tanto para profesores, estudiantes, secretarias y a toda la comunidad universitaria, ya que permite a los mismos obtener y visualizar sus datos referentes a su historial de calificaciones, y toda su documentación de forma eficiente.

Actualmente la F.A.F.I trabaja con una plataforma llamada SAI (SISTEMA ACADÉMICO INTEGRADO) donde solo las personas encargadas pueden disponer y tener acceso a todos los datos de los estudiantes de forma segura.

La presente investigación está enfocada en determinar los distintos problemas de la interconectividad y la seguridad de datos, que se presentan por la indebida conexión de equipos no autorizados, y a las ves mal configuradas, y la compartición del ancho de banda dentro de la facultad no es muy estable y los más afectados son los estudiantes, docentes, y los distintos departamentos que se encuentran dentro de la facultad.

El estudio de la interconectividad de la F.A.F.I ha presentado algunos tipos de inconvenientes, trabaja con el protocolo ipv4 y tiene 100 MB para toda la facultad lo cual no está distribuido de forma equitativa para toda la facultad y el principal inconveniente es cuando se realizan descargas de archivos de gran tamaño el ancho de banda es consumido por la descarga y esto causa que la interconectividad de toda la facultad comience a fallar.

II. DESARROLLO

La seguridad de datos es la que se encarga de proporcionar protección a la información de ataques no autorizados que pueden perjudicar a la institución. Los ataques pueden afectar la utilización de los equipos, la integridad de los datos y a la vez comprometer su confidencialidad.

Actualmente la seguridad de datos describe las medidas de defensa de toda la reserva de la información que se encuentra almacenada dentro de la institución, que pueden ser atacadas de manera imprevistas para actos maliciosos y para una posible alteración.

Este trabajo mantiene la línea de investigación de procesos de transmisión de datos y telecomunicaciones.

La interconectividad es el medio de entrada entre varias redes que se encuentran acopladas entre sí y sus principales características son:

- La compartición de recursos.
- Administración de recursos de otras redes.
- Aumento de cobertura.

La interconectividad está avanzando, y demanda que los ingenieros y las personas estén capacitados de acuerdo con los avances de ellos, para que puedan diseñar e instalar los equipos y aplicaciones de manera adecuada para que no hubiera fallas de conectividad en un futuro.

El presente caso de estudio fue fundamentado en la investigación de campo, la observación en el sitio, entrevistas a docentes de la facultad y al departamento de Tics de la universidad, esto dará evidencia de la importancia de la seguridad de los datos y la interconectividad. A partir de un sitio, para separar los elementos de la indagación y así llegar a un análisis de inspección y prevención.

Una vez realizado un análisis de la problemática y haber indagado uno de los principales problemas que se encuentran en la facultad sobre la interconectividad y la seguridad de los datos es que no hay controles ni reglas que permitan que la información este de manera segura ya que no dispone de ninguna medida para su protección.

El problema es que la gran parte de los puertos se encuentran abiertos por lo cual están propensos a posibles ataques, manipulación de los datos.

Estamos en una sociedad que avanza diariamente con los avances de la tecnología, y con los nuevos dispositivos y aplicaciones que se encuentran en el mercado, que les permitan mantener su información de manera segura, confiable, y así estar siempre alerta de posibles fallas o ataques.

De acuerdo a entrevistas realizadas los problemas de interconectividad y seguridad de datos se producen por la indebida conexión de equipos que no están configurados debidamente, y esto provoca bucles y a la vez perdidas paquetes y a la vez producía lentitud en los servicios.

Para determinar estos problemas se utilizó un firewall llamado SOPHOS UTM que fue creado para facilitar la protección total de las instituciones o empresas.

SOPHOS UTM nos permite detectar:

- Al instante los riesgos
- Detener amenazas de origen desconocido.
- Aislar los sistemas que están siendo atacados.

(Sophos, 2018)

Ilustración 1(Sophos UTM)

(Sophos UTM, 2018)

Sophos nos permite eliminar todo el programa malicioso que detecte o aísla los dispositivos que estén en peligro para evitar daños, una de sus ventajas es que puede bloquear vulnerabilidades de aplicaciones, internet, direcciones web, códigos maliciosos. (Sophos, 2018)

Si ocurriera algún inconveniente con los equipos que se encargan con el tráfico de red existe la posibilidad de pérdida de paquetes, y las principales causas son conexiones en deterioradas, fallas en los equipos, fallas en los router.

Los datos que circula a través de los múltiples terminales y enlaces. Si uno de estos nodos, se localiza bajo el total de su cabida se distribuye una cola de espera en donde la información pasa de una forma más pesada, alcanzando a descartarse después de un determinado tiempo. En la diferencia de los cuellos de botella es que se involucra un único lugar de congestión, sino que puede ser una dificultad general. (Andres, 2017)

La aparición de los bucles de tráfico de red de comunicación origina una perdida innecesaria de recursos de red y un aumento también innecesario de retardo. (Muñoz)

La facultad no consta con un firewall que controle el acceso de datos, por lo que se generan los bucles, intermitencia, lentitud en los servicios, ya que un firewall es el que controla el medio de entrada y salida del tráfico de datos siguiendo unas determinadas reglas que los administradores pueden establecer.

Básicamente la función principal que realiza un firewall es brindar protección a los dispositivos, servidores, equipos conectados a una determinada red frente accesos no esperados, que puedan obtener de manera ilícita la información e inclusive oponerse a los servicios de la red ya establecidos.

Los cortafuegos (firewall) consiguen crear el perímetro y también crear zonas de la red a las que se pueda acceder desde fuera sin comprometer la seguridad de la red interna. Estas zonas son las DMZ, que son trozos de red donde conectan los servidores que van a ser públicos,

como las páginas web corporativas, controlando totalmente el acceso a las zonas más interna de la red de la organización. (Moreno, 2015)

Los DMZ según Gabriel Díaz, Ignacio alzorriz, Elio San Cristóbal y Manuel Alonso dice que este este contexto hay que introducir lo que es un DMZ o zona desmilitarizada, que es una red directamente enlazada con el cortafuegos que esté utilizando.

DMZ

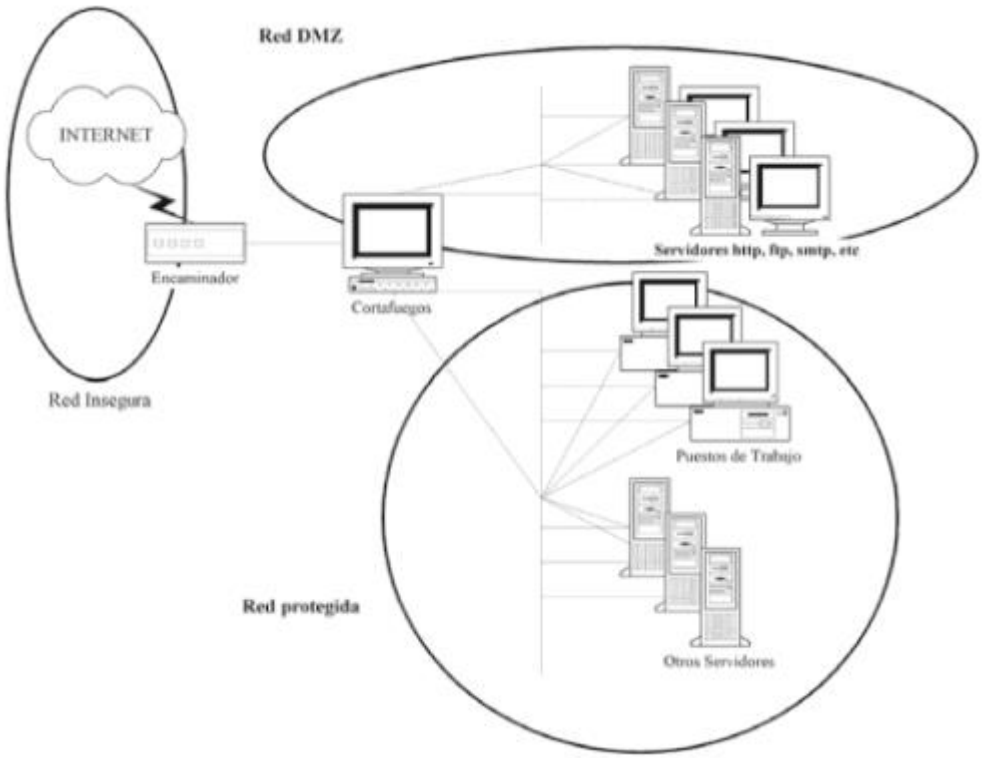

Ilustración 1(Topología de una DMZ típica)

Fuente: (Diaz , Alzorriz , Ruiz, & Castro, 2014)

Los cortafuegos son una parte fundamental de la red ya que fueron creados para bloquear la vía no autorizada, y a la vez nos admite cifrar, rechazar, pasar el tráfico entre diferentes terminales de red.

Firewall es un sistema que protege a un computador o a una red de computadores contra ataques o intrusiones originadas desde Internet u otras redes. Los firewalls se encargan de filtrar los paquetes que se intercambian a través de Internet. (SALGADO, 2017)

Dentro de la seguridad de datos encontramos algunas vulnerabilidades como:

La suplantación de IP son ataques de suplantación de la identidad, siendo una de las más conocidas la denominada IP Spoofing (enmascaramiento de la dirección IP), por este medio el atracador logra modificar la cabecera de los paquetes enviados a un explícito sistema informático para fingir que proviene de un dispositivo distinto al que realmente lo ha originado. (Vieites, 2014)

El principal problema que se presenta en la facultad sobre suplantación de IP se debe a la utilización de los router en los distintos cursos, ya que se debe a que los estudiantes le colocan una determinada dirección IP, pero no se dan cuenta que esa dirección Ip ya ha sido ocupada en otros departamentos y esto ocasiona que falle la conexión constantemente.

Arquitecturas inseguras, una red mal configurada da muchos puntos de acceso a los atacantes, para que puedan acceder a todos nuestros datos de manera fácil.

Servidores centralizados, es una forma para reducir gastos porque ponen a un solo computador a afianzar todos los servicios, esto puede ser beneficioso ya que se pueda manejar fácilmente y a la vez esa máquina que tenemos como servidor se ve comprometida a alguna falla, dejaría a la red totalmente indefensa, y dejaría la información propensa a la manipulación.

La facultad no cuenta con servidor centralizado dentro de ella, ya que todos los servidores se encuentran en el área de las Tics de la Universidad.

Ataques de Denegación de Servicio (DoS) tienen la finalidad de provocar que un servicio o recurso sea inaccesible para los usuarios legítimos. Este tipo de ataques pueden provocar:

- Parada de todos los servicios de una máquina.
- La máquina sólo puede dar determinados servicios.
- La máquina no puede dar servicio a determinados usuario.

Los ataques DoS se pueden llevar a cabo de diferentes formas y cubren infinidad de servicios. Existen tres tipos básicos de ataque:

- Consumo de recursos limitados.
- Destrucción o alteración de datos.
- Destrucción o alteración física de componentes de la red.

Ejemplos de ataques DoS

- Consumo de ancho de banda:
  - Smurf Attack: Este ataque se basa en mandar un gran número de peticiones hechas (ICMP) a direcciones de Broadcast usando una IP de origen falsa. Esto provoca que la IP de origen sea inundada con multitud de respuestas.
  - ICMP Ping Flood: En este ataque se inunda a la víctima con paquetes ICMP Echo Request.
  - Fraggle Attack: Es similar al ataque Smurf pero en este caso se envía tráfico UDP en lugar de ICMP.

- Ataques a la conectividad
  - SYN Flood Attack: Consiste en enviar muchos paquetes TCP/SYN con la dirección de origen falseada. Esto provoca que el servidor espere las respuestas que nunca llegan, provocando un consumo elevado de recursos que afectan al rendimiento del servidor. (Bermejo, 2007)

Vulnerabilidad de servicios

El atacante busca una abertura en el servicio de red, por el cual comenzar hacer los ataques y así comprometer a toda la red.

- Vulnerabilidades de nivel físico se trata del acceso no autorizada a los dispositivos de red que pueden ocasionar daños al equipo.
- Vulnerabilidad de enlace a datos es la que de dirigir todo el direccionamiento y la localización de errores.

III. Conclusiones.

- El presente estudio que se realizó en la Facultad de Administración, Finanzas e Informática, dará a conocer los distintos problemas de interconectividad y seguridad de datos y una de las causas es la indebida conexión de equipos no autorizados. Interconectividad

- Una de las medidas que se puede emplear para mejorar la interconectividad y la seguridad, es que la Facultad de Administración, Finanzas e Informática se aislé a través de un firewall. Y que se cree un equipo intermedio donde llegue la fibra óptica de la data center y así crear una red interna solo para la facultad y ahí ya establecer todas las reglas, controles proxy, control parental, etc.

- La F.A.F.I sostiene problemas de interconectividad, debido a la utilización de equipos no autorizados como los router que no se encuentran debidamente configurados, y eso causa inconvenientes como interferencia, perdida de paquetes, bucles, por esos motivos el departamento de sistema opto para evitar los distintos problemas con los router dentro de la facultad que se los lleven a ellos para la debida configuración.

ENTREVISTA

1.- Utilizan medidas de seguridad para la protección de datos dentro de la facultad.

Sí ☐ No ☐

2.- Actualmente en la F.A.F.I se aplican reglas de seguridad para la protección de los datos

Sí ☐ No ☐

3.- El cableado estructurado de la facultad se encuentra en óptimas condiciones.

Sí ☐ No ☐

4.- Que problemas cree usted que existen en la red dentro de la facultad.

- ✓ Puertos abiertos ☐
- ✓ Bucles ☐
- ✓ Indebida conexión de equipos ☐
- ✓ Ancho de banda insuficiente ☐

ENTREVISTA

1.- La Facultad de Administración, Finanzas e Informática cuenta con un firewall de seguridad.

Sí ☐ No ☐

2.- El firewall SOPHOS UTM nos garantiza la protección de total de la institución.

Sí ☐ No ☐

3.- El firewall SOPHOS UTM nos permite detectar:

……

……

……

……

4.- Cree conveniente que los estudiantes coloquen router en las aulas sin la debida supervisión del departamento de sistema.

Sí ☐ No ☐

Linkografía

Andres, C. (03 de mayo de 2017). Obtenido de https://blog.pandorafms.org/es/perdida-de-paquetes/

Gomez, A. (27 de Julio de 2018). *Ceupe.* Obtenido de Ceupe: https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html

Mifsud, E. (26 de Marzo de 2012). *Observatorio Tecnologico.* Obtenido de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Muñoz, A. A. (s.f.). *Teleinformatica y redes del computador.*

ocampo, v. m. (3 de Marzo de 2012). Obtenido de http://lyndziy.blogspot.com/2012/03/1.html

Rangel, I. (29 de Abril de 2015). Obtenido de http://www.udg.mx/es/noticia/la-interconectividad-puede-poner-en-riesgo-la-privacidad-de-una-sociedad-envuelta-en-la

Sophos. (12 de 08 de 2018). Obtenido de https://translate.google.com.ec/translate?hl=en&sl=en&tl=es&u=https%3A%2F%2Fwww.sophos.com%2Fes-es%2Fproducts%2Fnext-gen-firewall.aspx

Sophos. (12 de 08 de 2018). Obtenido de https://www.sophos.com/es-es/products/endpoint-antivirus.aspx

Sophos UTM. (12 de 08 de 2018). Obtenido de https://www.sophos.com/es-es/products/unified-threat-management.aspx

Bibliografía

Moreno, J. Z. (2015). *Ciberdiccionario:Conceptos de ciberseguridad en lenguaje entendible.*

Andreu, J. (2010). *Servicos en red.* Editex.

Diaz , G., Alzorriz , I., Ruiz, E., & Castro, M. (2014). *Procesos y Herramientas para la seguridad de datos.* Madrid.

Carpentier, J. F. (2016). *La seguridad informatica en la PYME.* ENI.

SALGADO, L. E. (2017). *IMPLEMENTACIÓN DE UN UTM (UNIFIED THREAT MANAGEMENT) PARA LA SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD PONTIFICIA BOLIVARIANA SECCIONAL MONTERÍA.*

Vieites, A. G. (2014). *Enciclopedia de la seguridad informatica.* Madrid.

Comer, D. E. (2015). *Redes de computadoras e internet.*