GESTION DE SEGURIDADES EN REDES DE COMUNICACIONES: ANÁLISIS DE SEGURIDAD EN LA RED DE DATOS DE LA FIEC

Daniel Efrén Pineda Mejillones[1], Edgar Leyton[2]

[1]Ingeniero Eléctrico, Especialización Electrónica 2004
[2]Director de Tópico, Ingeniero Eléctrico, Especialización Electrónica, Escuela Superior Politécnica del Litoral 1990, Profesor de la ESPOL desde 2001.

RESUMEN

Este proyecto está enfocado al análisis y aplicación de herramientas de gestión de seguridad informática y en los criterios que se deben seguir para mantener la seguridad en una red de datos. La aplicación de estas herramientas se la ejecuta en la red de datos de la Facultad de Ingeniería en Electricidad y Computación de la ESPOL con el objetivo de verificar si existe algún tipo de vulnerabilidad en la plataforma de los sistemas operativos de los servidores principales.

INTRODUCCIÓN

En cuestión de seguridad informática, no está dicha la última palabra; cada vez los piratas informáticos, conocidos como "*hackers*" desarrollan técnicas avanzadas para tratar de evadir los sistemas de protección de redes. Sin embargo, siempre hay que estar un paso mas allá y eso depende de la iniciativa de las personas encargadas de la administración de la red.

Se eligió a la red de la FIEC para poder implementar herramientas que ayuden al administrador a detectar o controlar si los recursos de la red (servidores principalmente) son propensos a sufrir un tipo de ataque por alguna vulnerabilidad en el sistema operativo de los mismos y también para controlar si existe algún tipo de tráfico en la red que tenga un patrón de ataque.

El objetivo de este proyecto es brindar a la FIEC un análisis de la seguridad de la red y recomendar diseños en la topología que incluyen equipos y herramientas que la protejan no solo de posibles ataques desde Internet sino también de ataques que puedan provenir de algún usuario en la misma red interna.

1. QUÉ ES UN FIREWALL?

Un firewall es un medio que sirve para regular el acceso a la red de computadoras de una organización. El papel de un firewall en una red de computadoras es controlar el acceso y registrar os intentos de acceso. Para ello, consulta la siguiente información: la dirección IP del host que origina la comunicación, la dirección IP del host destino y la información acerca del servicio solicitado. El firewall decide entonces, si permite o no la comunicación de acuerdo a las reglas o políticas de seguridad configurada por el administrador del firewall.

2. QUÉ SON LOS SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS)?

Los sistemas de detección de intrusos ayudan a los sistemas de computadoras a preparase y actuar ante eventuales ataques informáticos. Estos sistemas cumplen este objetivo recolectando información de diferentes fuentes de sistemas y de redes, analizan la información tratando de encontrar síntomas de problemas de seguridad. En algunos casos, los sistemas de detección de intrusos permiten al administrador de la red responder (en tiempo real) a estos intentos de ataques.

3. AMENAZAS REALES PARA LA INTRANET

Sin duda alguna, la identificación de los riesgos de seguridad para una Intranet, tal como se lo ha expuesto anteriormente, proporciona un sólido punto de partida para decidir si, en verdad, es necesario un firewall. Y como hemos sugerido, si piensa conectar una Intranet al ámbito público de Internet, probablemente decidirá que necesita un firewall.

Sin embargo, una vez que se llegue a esta conclusión, el administrador deberá responder a nuevas preguntas sobre las amenazas reales para su Intranet y la mejor manera de contrarrestarlas. Es decir, tendrá que determinar los tipos de ataques a la seguridad que deben evitarse, la forma como se integrará el firewall a la red y la disposición y organización de los diversos componentes del mismo.

4. BREVE DESCRIPCIÓN DE ALGUNOS ATAQUES PROCEDENTES DE INTERNET

Esta sección quiere demostrar lo fácil que resulta entender las estrategias básicas asociadas a ataques de los piratas informáticos conocidos como “*hackers*”. Los administradores de la red deben reconocer los principios asociados a los ataques

procedentes de Internet a fin de tomar una decisión apropiada respecto a los equipos de seguridad con los que cuenta su red, así como los riesgos que con éstos se pretende atenuar. Debido a que es imposible tratar íntegramente todas las amenazas procedentes de Internet, nos centraremos en los ataques más representativos.

4.1. Ataques de negación de servicio (Denial of Service).-

El siguiente gráfico ilustra lo que los usuarios de Internet pueden hacer. Ponemos como ejemplo, un servidor de correo electrónico (este servicio es uno de los blancos más habituales de ataque por negación de servicio). Prácticamente todos los usuarios que cuentan con una dirección de correo electrónico divulga su dirección a cualquier persona interesada en conocerla. Este tipo de ataque simple puede realizarse manualmente o mediante un programa que envía correo repetidamente a la víctima hasta que el sistema de ésta es incapaz de gestionar el volumen.

Lo cierto es que no existen muchas maneras eficaces de evitar los ataques de negación de servicio. Sin duda, desactivar la recepción de correo electrónico no es una posibilidad (la solución es peor que el problema ya que se interrumpe el servicio para toda la organización). Asimismo, regular los mensajes de correo para reducir el riesgo de sufrir ataques de este tipo no es sencillo, además de que interfiere en el flujo normal de correo. Existen firewalls de algunos fabricantes que permiten limitar el número de conexiones a los sistemas anfitriones internos, lo cual puede ser una de las varias soluciones posibles.

Por cierto, las amenazas de negación de servicio no están limitadas sólo al uso de correo electrónico. Cualquier tipo de servicio al que confían acceder rápidamente los usuarios es potencialmente vulnerable a este ataque.

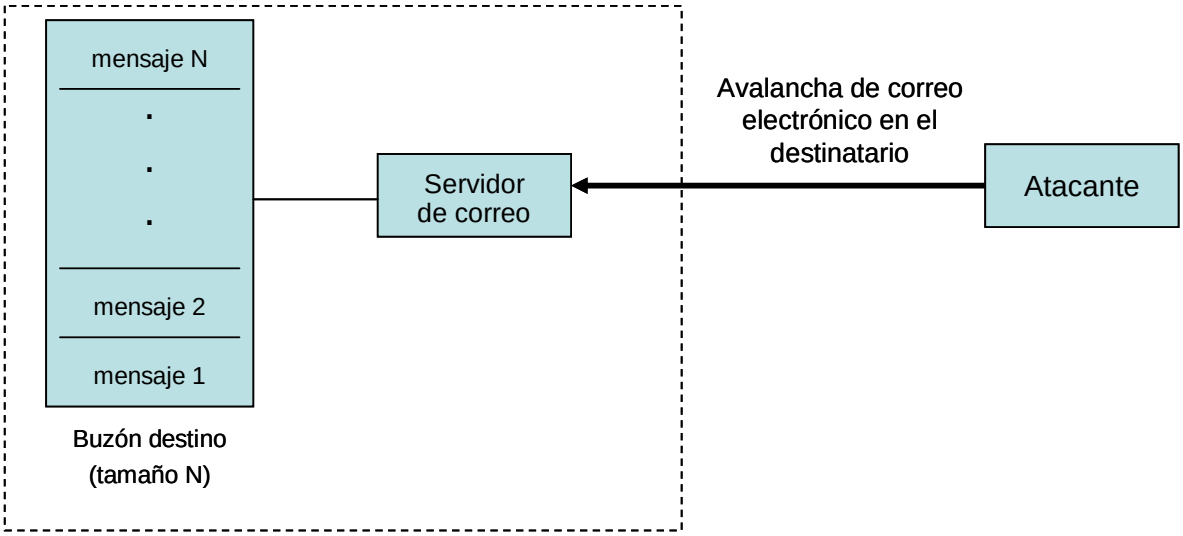

Figura 1. Diagrama de bloque que representa un ataque del tipo Negación de Servicio

4.2. Aspiración de paquetes en la red (*Packet Sniffing*)

Cuando una computadora está conectada a una red de área local (LAN), como una Ethernet, es vulnerable a ataques de este tipo en los que alguien puede "escuchar" los datos que fluyen por la red. Los programas llamados aspiradores de paquetes (*sniffers*) capturan paquetes que recorren la LAN y los presentan de forma legible.

El remitente y el destinatario de esta información probablemente no lleguen a saber nunca que ha sido "pinchada". Los administradores de la red han utilizado los sniffers durante muchos años como una útil herramienta de diagnósticos de problemas en la red. Si su red LAN está conectada a Internet, es posible que extraños a la misma red local puedan realizar una aspiración de paquetes, atacando con éxito solamente uno de los sistemas anfitriones de la red.

4.3. Ataque por suplantación de IP (*IP Spoofing*)

Otro tipo habitual de ataque en Internet consiste en los intentos de suplantar la dirección IP de una víctima. Un intruso puede utilizar la técnica conocida como *IP spoofing* para personificar la identidad de un host para aplicaciones o servicios que utilizan direcciones IP fuente o destino para autenticación. Un ataque *IP spoofing* ocurre cuando un intruso fuera de la red de la organización pretende ser un host confiable (este host confiable puede estar dentro o fuera de la red de la organización). El spoof utiliza una dirección IP que está dentro del rango de

direcciones de la red o puede utilizar una dirección IP externa pero que está autorizada y es confiable para proveer acceso a recursos de la red. La siguiente figura ilustra un esquema de suplantación de IP.

En la figura No.2 un sistema externo presenta 10.12.1.1 como su dirección IP, la cual resulta ser la dirección de un usuario interno. Si el firewall o router realiza el filtrado de paquetes solamente según la dirección IP, es posible que los datos entren dentro de la red.

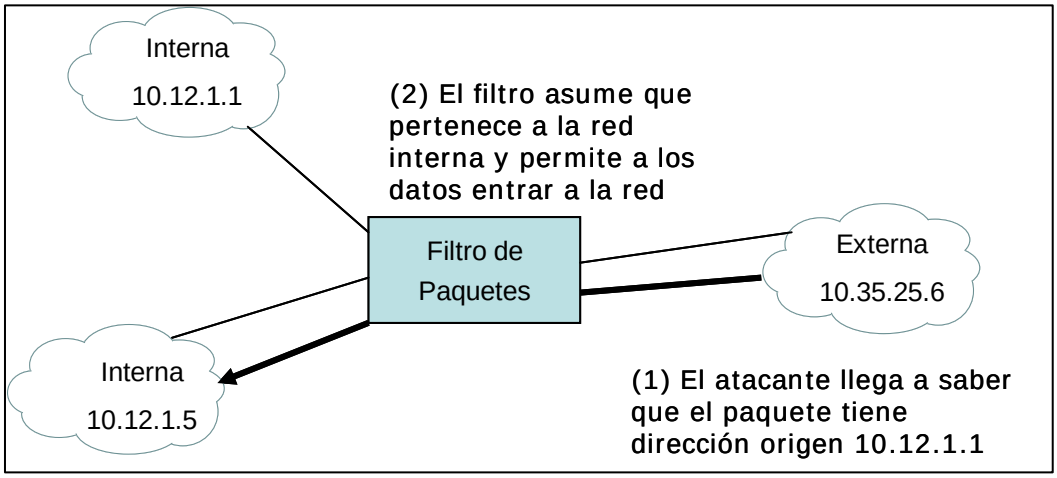

Figura 2. Ataque por suplantación de IP

5. SITUACIÓN ACTUAL DE LA RED DE DATOS DE LA FIEC

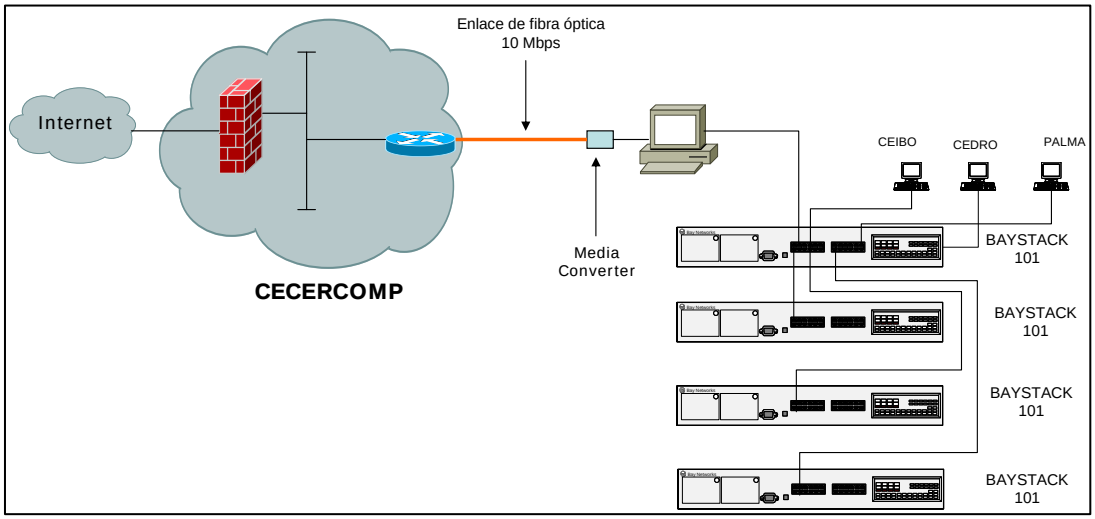

Figura 3. Diagrama de la red de datos de la FIEC

La figura 3 representa la estructura general de red de la FIEC. La estructura de red de la FIEC es muy sencilla, en lo que se refiere a equipos de conectividad cuentan con 4 hubs Bay Networks de 24 puertos RJ-45 que trabajan a 10 Mbps. La conexión entre los hubs es en cascada, es decir, desde un hub principal se distribuye la señal de datos hacia los tres hubs restantes por medio de cable UTP; con esto tenemos lo que se conoce como un dominio de colisión y un dominio de broadcast (dominio de difusión).

Existe un computador que realiza la función de ruteador utilizando dos tarjetas de red separando la red de la FIEC del resto de la red del campus de la ESPOL.

En esta red constan los puntos de red para los laboratorios, para las oficinas de los profesores y para la oficina de los administradores de la red con los servidores principales.

El equipo de frontera entre la red LAN de la FIEC y el resto de la ESPOL es un PC con dos tarjetas de red para separar la red de la FIEC del resto de la red del campus, esta PC actúa como ruteador y como gateway (puerta de acceso) para la facultad.

El medio de transmisión para el acceso a la ESPOL es fibra óptica monomodo a una tasa de transmisión de solo 10 Mbps, por lo que está desperdiciando la mayor parte de los beneficios de tener un enlace de fibra óptica entre dos localidades.

Esta fibra llega hasta las oficinas de CECERCOMP que es la entidad que administra la red de datos de la ESPOL, es en CECERCOMP donde se concentra todos los requerimientos por consultas y servicios de Internet. Para el caso de la FIEC, CESERCOMP actúa como un proveedor de última milla puesto que los servicios que brinda la facultad son totalmente independientes de CECERCOMP.

El protocolo de comunicación TCP/IP es el utilizado en la red. El esquema de direccionamiento IP corresponde a la red 200.9.176.0 con máscara de subred 255.255.255.0; esto quiere decir que todos los hosts cuya dirección IP comience con los tres primeros octetos 200.9.176 pertenecerán a la red de la FIEC.

6. INSTALACIÓN DE HERRAMIENTAS DE GESTIÓN DE SEGURIDAD Y REALIZACIÓN DE PRUEBAS DE DETECCIÓN DE VULNERABILIDADES

Es muy importante para el administrador de cualquier red de datos realizar el monitoreo de la actividad de su red, no solo para verificar el correcto funcionamiento de toda la infraestructura que la conforma, sino para controlar el correcto uso de todos los recursos que esta ofrece a los usuarios.

En el desarrollo de este proyecto, hemos enfocado nuestras pruebas utilizando dos herramientas de gestión de seguridades: CISCO SECURE SCANNER y ETRUST INTRUSION DETECTION. Ambas herramientas están dentro del grupo de herramientas de reconocimiento ya que con ellas se puede averiguar los hosts que están disponibles en una red (hosts activos) y saber detalles de los mismos, es decir, si son servidores, ruteadores, switches, plataforma de sistema operativo, servicios TCP-IP disponibles, etc.

Ambas herramientas fueron instaladas y puestas en funcionamiento en la red de la FIEC. El objetivo principal de las pruebas que se realizadas es detectar vulnerabilidades en la plataforma de sistema operativo de los servidores principales de la red, verificar el funcionamiento de la herramienta de detección de intrusiones en la red y en base a estas pruebas, poner a consideración del administrador de la red las sugerencias que se deben seguir para mejorar la seguridad en los recursos de la red.

6.1. Características del Cisco Secure Scanner

Podemos mencionar las siguientes:

- **Descubrimiento de Vulnerabilidades.-** El scanner descubre puntos débiles de seguridad en la red antes que algún intruso pueda explotarlas. La herramienta permite automáticamente compilar un inventario de los dispositivos y servidores en la red; luego utilizando una base de datos, el scanner identifica las vulnerabilidades asociadas con servicios de red para mostrar al usuario en una tabla todas las deficiencias en los servicios de red de los dispositivos que son objeto del análisis.

- **Detalle de las vulnerabilidades.-** Esta herramienta provee detalles sobre cada vulnerabilidad así como del host en el que ha sido detectado dicha

falencia (el host vulnerable), la debilidad en el sistema operativo, una descripción de la vulnerabilidad y las acciones que se deben tomar para corregir la debilidad.

- **A qué redes realizar este análisis.-** Se puede utilizar esta herramienta para toda red basada en el protocolo TCP/IP. La herramienta puede realizar un scann a redes conectadas a Internet así como también redes aisladas.

6.2. Características del eTrust Intrusion Detection

Esta herramienta ofrece las siguientes características:

- **Control de Acceso a la Red –** eTrust Intrusion Detection utiliza una base de reglas para definir a los usuarios que pueden acceder a determinado recurso en la red, asegurando solo acceso autorizado a recursos de la red.

- **Motor de Antivirus Avanzado –** un motor antivirus detecta el tráfico en la red que contenga virus de computadoras. De esta manera se protege al usuario de la descarga inconsciente de archivos infectados con virus. Las actualizaciones de virus se encuentran disponibles en el sitio Web del fabricante.

- **Base de Datos con Patrones de Ataques –** eTrust Intrusion Detection de manera automática detecta patrones de ataques en el tráfico de la red incluso mientras el ataque está en marcha. Existe una base de ataques que se actualiza regularmente y que se encuentra disponible en el sitio Web del fabricante.

- **Tecnología de Olfateo de Paquetes –** eTrust trabaja u opera en modo “disimulado”, manteniéndose indetectable para los atacantes.

- **Bloqueo por URL –** Los administradores pueden designar las direcciones URL a las que los usuarios no pueden acceder previniendo la navegación no productiva.

- **Registro de la Utilización de la Red –** Esta herramienta permite al administrador de la red tener un registro de logs de la actividad que los

usuarios le han dado a la red; este registro puede ser por aplicaciones, por usuarios, etc. Esto ayuda a mejorar la planeación de las políticas de la red.

Los resultados de las pruebas realizadas brindan información crítica que podría ser utilizada de manera no conveniente a los intereses de la FIEC. Por razones de confidencialidad, omitimos estos resultados.

7. SUGERENCIAS REALIZADAS A LA FIEC PARA LA MEJORA EN EL RENDIMIENTO Y SEGURIDAD DE LA RED.

Con el análisis de la topología de red de la FIEC podemos emitir los siguientes puntos para la mejora en la estructura de la red.

- Implementación de un equipo con funcionalidad exclusiva de firewall.
- Implementación de una zona desmilitarizada para servidores públicos.
- Implementación de NAT para optimizar el uso de direcciones públicas.
- Implementación de equipos o programas para el monitoreo de posibles ataques a la red interna desde Internet y desde la misma red de la FIEC.
- Distribución de carga para los servidores, es decir, no acumular todos los servicios en un solo equipo.
- Cambio en los equipos de conectividad final por otros de mejor rendimiento y con capacidad de administración remota por SNMP.
- Implementación de una herramienta de gestión de redes para el control y monitoreo de los equipos de conectividad y de los servidores críticos.
- Movilización del rack donde se encuentran los equipos de conectividad a un sitio más seguro y de acceso restringido junto con los servidores críticos.

El siguiente gráfico indica el esquema de red sugerido a la FIEC

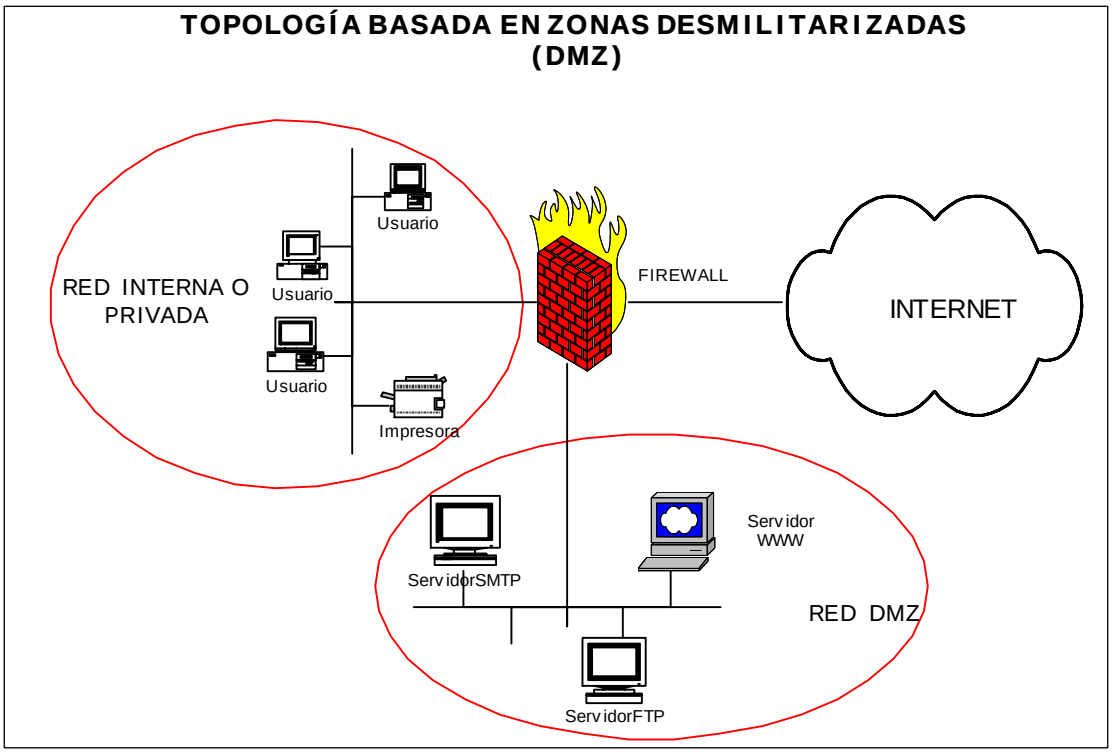

Figura 4. Topología de red sugerida a la FIEC

En el gráfico se aprecia una arquitectura “three homed” con el firewall como equipo central de control de tráfico con tres interfaces de red: red externa, red desmilitarizada y red interna.

Los servidores con servicios públicos hacia Internet instalados en la red DMZ, los usuarios en la red interna y en la red pública la conexión directa hacia el dispositivo de conexión a Internet.

Este tipo de configuración es la ideal para el ambiente de trabajo en la FIEC considerando la gran cantidad de usuarios que tiene la facultad; en este diseño se ha puesto mucho énfasis en protección a los servidores de la red DMZ ya que no solo los ataques pueden provenir de Internet, sino también desde la misma red privada por lo que es necesario mantener un alto nivel de seguridad para eso equipos críticos.

8. CONCLUSIONES

1. La topología de red que brinda un mayor nivel de seguridad a la FIEC es basado en redes DMZ, aislando física y lógicamente los servidores que brindan servicios de Internet del resto de computadoras de la red. Con

esto se consigue seguridad a servidores que brindan servicios internos (base de datos, servidores de aplicación, etc.) y también restringir el acceso a los servidores públicos solo por los protocolos necesarios. Esto se lo define en las reglas de acceso en el firewall y con el criterio del administrador de la red.

2. Si bien es cierto, el objetivo de este proyecto no es el de evaluar productos o herramientas de firewall, recomendamos implementar un equipo dedicado a las funciones de firewall en la red de la FIEC, el actual dispositivo no brinda las características competas de un buen firewall. En el capítulo V de este proyecto se indican firewalls basados en hardware y software podrían ser considerados como alternativas por la Facultad.

3. El administrador de la red debe contar con herramientas como los sistemas IDS (detección de intrusiones) para el monitoreo de tráfico sospechoso en la red. Recomendamos la herramienta ETRUST INTRUSION DETECTION de la casa fabricante COMPUTER ASSOCIATES que se ha utilizado en las pruebas realizadas en este proyecto. Esta herramienta demostró tener un nivel de eficiencia muy bueno y además se puede implementar filtrado del tráfico Web evitando el acceso a páginas en Internet con contenido nocivo para los usuarios (sitios de pornografía, de juegos, de descarga de archivos mp3s, etc.) que no contribuyen al objetivo de investigación y educación que debe tener Internet en las entidades educativas y que además consumen ancho de banda.

4. Es de vital importancia mantener actualizado la herramienta de antivirus que tengan los servidores y estaciones de trabajo Muchos de los ataques se deben a la ejecución de virus “troyanos” en computadoras y servidores y que brindan al *hacker* la posibilidad de tomar control de determinado host para tratar de ingresar a servidores más importantes. Además, al mantener actualizado las herramientas de antivirus, brindamos mayor seguridad a la información almacenada en los servidores.

5. Finalmente, recomendamos que se tenga actualizado el sistema operativo de servidores y estaciones de trabajo con los últimos parches y actualizaciones (*fixes*) de seguridad para disminuir la probabilidad de ser víctimas de ataques de usuarios externos e internos.

REFERENCIAS

1. M. Wenstrom, Managing Cisco Network Security (Indianápolis, Cisco Press, 2001), pp.6-33
2. E. Amoroso y R. Sharp, Seguridad en Internet e Intranet (Madrid, Prentice-Hall, 1997), pp.29-38

Ing. Edgar Leyton
Director de Tópico