UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ABRIL 2022 – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE FIN DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

DISEÑO DE UNA RED DE SEGURIDAD PERIMETRAL BASADA EN OPEN SOURCE PARA APLICACIÓN DE IDS E IPS PARA EL CONTROL DE AMENAZAS INFORMÁTICAS EN LA UNIVERSIDAD TÉCNICA DE BABAHOYO

EGRESADA:

FANI YUDID CABRERA VÁSQUEZ

TUTOR:

ING. IVAN RUBEN RUIZ PARRALES

AÑO 2022

RESUMEN

Mediante la presente investigación se pretende presentar el diseño de una Red de Seguridad Perimetral basada en Open Source para aplicación de IDS e IPS para el control de amenazas informáticas en la Universidad Técnica de Babahoyo, la cual permite proponer una propuesta de implementación para evitar ataques internos y externos que llegue a tener la institución, de manera que se garantice la confidencialidad, integridad y disponibilidad de los datos; por ende, se analiza de manera eficiente la información con la finalidad de que aunque los proveedores de las compañías de internet tengan un alto índice de vulnerabilidades en relación a la infraestructura de la red, especialmente en los equipamientos de la red central, estos deban evitar cualquier tipo de ataque que provengan desde la internet o desde su propia red interna garantizando la confidencialidad, integridad y disponibilidad de los servicios. El objetivo de la investigación es mejorar la seguridad de la red en la UTB evaluando la situación actual de la institución con sus respectivos requerimientos funcionales. Para la recolección de información fue preciso emplear la técnica de investigación la entrevista dirigida a Ingenieros; a su vez, este documento da paso a la obtención de información que es necesaria para mitigar amenazas informáticas en la institución.

El presente compendio investigativo da a conocer información confiable que ha sido obtenida por medio del uso de herramientas, con la finalidad de saber la situación actual de la red, y en este punto es donde se identifican las vulnerabilidades y sus posibles consecuencias que afectan a la red.

Palabras claves: Red de Seguridad Perimetral, IDS, IPS, Vulnerabilidades.

SUMMARY

Through this research, it is intended to present the design of a Perimeter Security Network based on Open Source for the application of IDS and IPS for the control of computer threats at the Technical University of Babahoyo, which allows proposing an implementation proposal to avoid internal attacks. and external that the institution may have, in a way that guarantees the confidentiality, integrity and availability of the data; therefore, the information is efficiently analyzed so that although the providers of internet companies have a high rate of vulnerabilities in relation to the network infrastructure, especially in the equipment of the central network, they must avoid any type of attack that comes from the internet or from its own internal network, guaranteeing the confidentiality, integrity and availability of the services. The objective of the research is to improve network security at UTB by evaluating the current situation of the institution with its respective functional requirements. For the collection of information, it was necessary to use the research technique of interviewing Engineers; in turn, this document gives way to obtaining information that is necessary to mitigate computer threats in the institution.

This investigative compendium discloses reliable information that has been obtained through the use of tools, in order to know the current situation of the network, and at this point is where the vulnerabilities and their possible consequences that affect the network are identified. net.

Keywords: Perimeter Security Network, IDS, IPS, Vulnerabilities.

INTRODUCCIÓN

La presente investigación está dirigida al diseño para la implementación de técnicas para elaborar una Red Perimetral basada en Open Source como una solución para mejorar la seguridad de la Red de la Universidad Técnica de Babahoyo, la cual se basa en la introducción de este instrumento informático para disminuir o evitar ataques para el control de amenazas informáticas en la institución, lo que resulta muy importante y fundamental para la protección de la información en un sistema de red moderna.

En este tiempo se debe tener muy en cuenta los componentes físicos y lógicos presentes en una red, ya que por el descuido se puede caer en el error de que esta información esta encriptada sin tomar en consideración amenazas o incidentes informáticos de la seguridad en las redes, ya que cada día son más comunes, costosos, menos extraordinarios y más masivos.

La Red de Seguridad Perimetral es un método de defensa en una infraestructura de red, la misma manera que permite defender la información de una institución del cual los recursos van a requerir acceso a Internet, pudiendo restringir y controlar qué datos ingresan o salen de la red, con privilegio al administrador de centralizar los puntos de ingreso, sin dejar el resto de servidores internos de la red para la protección de amenazas.

Para tal efecto, se debe estimar los recursos informáticos que son adecuados para las pasarelas que permiten realizar la interacción entre los usuarios de la Universidad Técnica de Babahoyo, sus funcionalidades de la Red de Seguridad y toda la infraestructura operativa de la institución.

Ante la propuesta tecnológica que se ha elaborado, tiene como fin proponer una topología de red teniendo en cuenta aspectos importantes que aseguren la seguridad perimetral de una red, por lo cual se decretan políticas de seguridad en la configuración de la red para evitar ataques internos y externos que llegue a tener la institución garantizando la confidencialidad, integridad y disponibilidad de los datos.

En el presente documento la característica primordial de esta investigación es implementar todo lo requerido para simular la práctica con respuestas eficientes a través de un diseño que permita cumplir los objetivos a la función de la red de seguridad de la UTB. Así mismo, para realizar esta investigación se identifican las vulnerabilidades y sus posibles consecuencias que afectan a la red.

La metodología usada en esta investigación es el método cualitativo con su respectiva técnica de investigación que es la entrevista y con las diferentes referencias bibliográficas se intenta obtener información importante que ayude a definir de una manera más clara el proyecto y la metodología de investigación a utilizar es la Deductiva.

La línea de investigación a utilizarse en el presente compendio investigativo es la de Sistema de Información y Comunicación, Emprendimiento e Innovación, y la Sublínea es redes y tecnología de software y hardware.

DESARROLLO

La Universidad Técnica de Babahoyo (UTB) es una universidad pública que está ubicada en la ciudad de Babahoyo, Provincia de Los Ríos. La UTB fue creada oficialmente el 5 de octubre de 1971 por el presidente de la República José María Velasco Ibarra, con cada una de las facultades de: Medicina, Veterinaria, Ciencias de la Educación e Ingeniería Agronómica, cuyas funciones fundamentales de este organismo son: Docencia, Investigación, Vínculos con la Comunidad y Gestión Institucional.

La UTB sostiene la tarea de producir, impartir y difundir una formación profesional eficaz y humanitaria por medio de funciones sustantivas, socialmente consientes, para perfeccionar las condiciones de vida de las personas y su entorno ambiental. Por lo que, cuenta con las siguientes facultades: Facultad de Ciencias Jurídicas, Sociales y de la Educación, Facultad de Ciencias de la Salud, Facultad de Informática Financiera y Administrativa, Facultad de Ciencias Agropecuarias, asimismo tiene la extensión Quevedo, la extensión El Ángel, que está ubicado en la provincia del Carchi.

Actualmente la institución tiene su sitio web oficial donde brinda información referente a ella que va dirigida a los estudiantes, docentes y personas en general, igualmente cuenta con un sistema académico integrado (SAI) que organiza, administra y tiene como objetivo ser la fuente de datos para toda la institución, por lo que se establecen los roles para cada usuario que tiene acceso a ella; también tiene una plataforma de aprendizaje llamada (Moodle) que le proporciona a los administradores y estudiantes un sistema integrado único y seguro para crear ambientes de aprendizaje personalizados.

El problema de Seguridad en la Red de la Universidad Técnica de Babahoyo

La problemática de la institución es identificar las vulnerabilidades ante amenazas informáticas en la Red de la Universidad Técnica de Babahoyo, de tal forma una vez identificados en esta investigación se basa en tratar la seguridad de la red de la manera más accesible, ya que no se cuenta con las herramientas necesarias para la detección de intrusos en la Red y así fortalecer su seguridad para no sufrir algún cambio en la información debido a ataques informáticos. Existen diferentes herramientas para mantener una óptima seguridad como son los firewalls, IDS e IPS.

De acuerdo a la entrevista realizada al Departamento de Sistemas de la UTB; por lo que, se identificó que actualmente la institución no cuenta con un Sistema de detección de intrusos; otro problema que se debe mencionar es que la Universidad tiene ataques informáticos y son: ataques de instrucción de acceso a los puertos que se tiene abierto, ataques DOS, ataques de virus en Red, ataques de malware de Red, ataques a los servidores de la Universidad que no se encuentran seguros; mencionar que el nivel de seguridad de la Red es intermedia lo que genera vulnerabilidades informáticas y para solucionar este detalle se debe obtener un firewall para poder configurar como IDS e IPS donde el resultado de la seguridad podría ser alta en la Red; hay que tener en cuenta que todos los días la institución tiene ataques informáticos, prácticamente las 24 horas ya que por minuto se llega a sufrir entre 400 a 500 ciberataques de IP, por lo tanto, se necesita una buena seguridad en la Red de la Universidad Técnica de Babahoyo; de forma que se pueda trabajar de manera segura y fiable.

Seguridad Perimetral

Esta seguridad se basa en proteger de todo sistema informático de una empresa del exterior, en otras palabras, componer un caparazón que deba respaldar todos los elementos sensibles a ataques dentro de un sistema informático. Significa que cada paquete de tráfico transmitido debe diseccionarse, analizarse y aceptarse o rechazarse en función de su riesgo potencial de seguridad para nuestra red.

Al realizar el diseño del sistema de seguridad perimetral es fundamental proponer un análisis de la situación actual de la red, pudiendo así saber cuál de los segmentos de la red de datos necesita más defensa; o sea, qué segmento de la red debe o no debe tener permisos para acceder a los datos, servicios de red o internet. Por lo tanto, se recomienda el uso de Open Source para la implementación del Firewall, IDS e IPS (INGENIERÍA Y TECNOLOGÍA, 2020).

Ilustración 1 Seguridad perimetral y Cortafuegos, Recomendaciones
Fuente: *https://www.micro.ai/blog/thingbots-the-rise-and-the-risk-to-iot-device-security*

Segmentación de Redes

Para la implementación de una Seguridad Perimetral se debe proponer una adecuada segmentación de la red a través de VLANs con sus respectivas direcciones IP. Al posee un registro de las VLAN e IPs empleadas en la red, la cual se pueden aplicar políticas a cada uno de los segmentos. A la hora de realizar una segmentación de red se debe tener en cuenta el posible incremento de la red de datos, para así poder fijar un pull de direcciones IP que proteja tanto la situación actual como el posible incremento.

Después de segmentar la red, es necesario configurar los equipos de red activos como Switches y Routers de Capa 2, si no hay Routers, hay que configurar un Switch de Capa 3 (Fernández, 2020).

Funciones para una excelente Seguridad Perimetral

Esta seguridad es la que protege tus redes y debe efectuar cuatro funciones primordiales:

– La seguridad resiste a ataques del exterior.

– Es aquella que identifica los ataques sufridos y así estar alertas de los mismo.

– Se aísla y divide los diferentes servicios y sistemas en función de su exhibición a ataques.

– Filtra y bloquea el tráfico, aprobando solo lo estrictamente necesario (Imagar Solutions Company, 2020).

Los objetivos de la Seguridad Perimetral

- Hacer frente a los ataques del exterior.
- Encontrar y reconocer los ataques informáticos recibidos y alertar sobre los mismos.
- Dividir sistemas y servicios conforme la superficie de ataque.
- Filtrar e impedir el tráfico ilegítimo (Grupo Atico34, 2021).

Herramientas de Seguridad Perimetral

Ya que se tiene una idea generalizada de cómo podría ser una seguridad perimetral informática, se va a detallar alguna de las herramientas específicas que se usan para reforzar su defensa y estas son:

Los Routers Borders

Como las puertas en el muro de un castillo, los Routers borders están ubicados en el borde del perímetro de la red y ayudan como guía para el tráfico entrante o saliente. Al establecer la frontera, comparte partes de las redes públicas y privadas.

Los Firewalls

Los cortafuegos son la serie de paredes interiores que se conduce como un filtro adicional para el tráfico entrante. Ellos deciden quién “o qué” debe o no debe verse afectado en un conjunto de reglas predefinidas.

De igual manera antes las otras herramientas mencionadas aquí, no pretenden ser la única línea de defensa de una institución, ya que deben utilizarse junto con otro software y dispositivos.

El Sistema de Detección de Intrusos (IDS)

El IDS es un sistema de alarma, ya que puede ser un solo dispositivo o una serie de dispositivos que monitorean la red en busca de actividad maliciosa o ataques a las políticas. Se diferencia de un firewall “cortafuego” en que tiene vigilado las intrusiones dentro de una red interna e informa un ataque desde dentro de la red.

El Sistema de Prevención de Intrusos (IPS)

A diferencia de un IDS que hace sonar la alarma sobre posibles amenazas informáticas, un IPS las detiene de manera automática según una lista de reglas preestablecidas; por ende, un sistema de prevención de intrusos es el "vigilante nocturno" ya que interviene para interceptar el tráfico entrante, bloquearlo, descartar paquetes de datos maliciosos o restaurar la conexión por completo.

El IPS proporciona una tarifa adicional por escaneo y seguridad interna, pero sin que intervenga de forma directa un administrador; por lo que, se considera también como un cortafuegos de próxima generación, que es principalmente una versión avanzada de un firewall más clásico, pero con la técnica adicional de impedir malware y usar la inspección profunda de paquetes (DPI) en línea (Hubbard, 2022).

Cómo gestionar la Seguridad Perimetral

La necesidad de gestionar o respaldar las redes privadas frente a posibles intentos de infiltración externa e interna debido a la interconexión de equipos informáticos en la red, la particularidad de algunos de ellos en concretos servicios correspondientes a la conexión de estos últimos a Internet para enseñarles a cualquier usuario.

Para el diseño y ejecución de la protección perimetral hay que considerar los diversos elementos que se utilizarán para el desarrollo de los controles de acceso. Por ello, los switches y routers son los encargados de segmentar el dominio de colisión y determinar los equipos que se ven sin necesidad de filtrar; por ende, Los switches son considerados elementos de seguridad ya que permiten la segmentación del dominio de colisión.

Uno de los elementos importantes en la seguridad perimetral son los routers de selección, ya que es un dispositivo de red encargado de encaminar paquetes de una interfaz a otra, empleando una serie de reglas de enrutamiento que serán indicados por configuración; por lo que, El enfoque de protección se centra, asimismo de la seguridad perimetral informática del sistema de prevención de intrusos (IPS), seguridad de redes inalámbricas, prevención de fugas de información o firewalls (cortafuegos) (Puente, 2018).

Ilustración 2 Cómo afecta la trasformación digital a la seguridad perimetral informática de la empresa
Fuente: https://www.cic.es/seguridad-perimetral/

Mejorar la Seguridad Perimetral

La seguridad perimetral es la integración de sistemas o pueden ser objetos para lograr la protección de un perímetro físico de la institución y sostener la disuasión de intrusión o detección de intentos de intrusión ante las amenazas informáticas. También, este tipo de seguridad perimetral llega a ser electrónica o mecánica; por consiguiente, su objetivo principal será mantener un determinado espacio 100% protegido y esto permite mejorar el perímetro de una institución como los siguientes: Detección, Demora, Evaluación y Respuesta (USS Seguridad Integral, 2021).

Funciones de la Seguridad Perimetral

- Parar los ataques ante una baja incidencia de falsas alarmas, tantas como sea posible.

- Hacer que se retrasen los ingresos potenciales y ganar tiempo e iniciar acciones de respuesta.

- Evaluar con precisión la amenaza para precisar la reacción ante cualquier ataque (ciberseguridad México, Fortinet México, seguridad de redes México, 2021).

Importancia de la Seguridad Perimetral

La importancia de la seguridad perimetral frente amenazas informáticas sigue creciendo y la información está expuesta a cualquier institución que cuente con los recursos adecuados para poder acceder a ella; por lo tanto; es necesario que la entidad tenga el control ante cualquier ataque informático (Morales, Toapanta, & Toasa, 2019).

Elementos de la Seguridad Perimetral

A continuación, los elementos que integran una seguridad perimetral, con el fin de cumplir los objetivos de protección.

- Routers fronteras.
- Firewalls (Cortafuegos).
- Sistema de Detección de Intrusos (IDS)
- Sistema de Prevención de Intrusos (IPS)
- Pasarelas (antimalware) y (antispam)
- Redes privadas virtuales (VPN).
- Software y servicios
- DMZ y Subredes controladas (Villalta, 2018).

Open Source

Open Source (Código abierto) no indica que el software sea gratuito; más bien, se refiere a que el usuario puede acceder al código fuente gratis; por lo que, una de las ventajas es que es posible promover la colaboración entre diversos usuarios de un programa de código abierto. Los usuarios pueden revisar y/o editar con total independencia y según sus necesidades. Aunque, hay más probabilidades de que los programas se vayan actualizando, no solo en relación a la usabilidad sino también en términos de seguridad y permiten a los usuarios corporativos e individuales la conveniencia de configurar todas las funciones de red fundamentales para un funcionamiento adecuado (Fernández, RZredeszone, 2022).

Seguridad en Open Source

- Identifica las Vulnerabilidades.
- Detecta el método vulnerable en la biblioteca.
- Vulnerabilidad y exposiciones comunes (CVE).
- Sistema Común de Puntuación de Vulnerabilidad (CVSS).
- Descubre Vulnerabilidades que no tienen CVE (Perez Padilla, 2020).

Riesgo en Open Source

Ante la aceptación y sus ventajas para la colaboración en el sector de las TICS, la utilización de Open Source tiene ciertas desventajas. Por su naturaleza, el software de código abierto no tiene obligación legal de protegerlo y carece de seguridad, soporte o garantías de contenido, aunque, según Red Hat el 85% de las entidades consideran que es lo más seguro posible. Otra razón en contra de lo que se menciona son los problemas de propiedad intelectual, puesto que, entre las más de 200 licencias disponibles del open source, existen diversas incompatibilidades. Por otro lado, hay que tener en cuenta que, al tratarse de un código asequible, sus vulnerabilidades serán de público conocimiento, manifestando a sus usuarios a ataques informáticos (EQUIPO COREMAIN, 2021).

Ilustración 3 Open Source ¿qué es y cómo funciona?
Fuente: https://www.icm.es/2020/01/22/open-source/

Vulnerabilidades en Open Source

Las vulnerabilidades en Open Source son conocidas por el público en general, así como por entidades como Open Web Application Security Project (OWASP) y National Vulnerability Database (NVD). Por lo tanto, mantener estos programas actualizados es un asunto muy importante, ya que hay posibilidades de que existan funcionalidades no deseadas en dichos programas, por lo que es fundamental configurarlo con los requisitos y permisos que necesitamos.

Al ser de código libre es susceptible de ser modificado por otros usuarios, es primordial descargarlo de fuentes y sitios webs seguros para prevenir sustos en forma de malware o troyanos. Y al no tener soporte directo de ningún fabricante; por lo que, todo dependerá de las circunstancias de cada proyecto, teniendo siempre en cuenta los beneficios y los riesgos.

- **Actualizar:** Es primordial estar al día, ya que los ciberdelincuentes aprovechan estas vulnerabilidades para realizar ataques informáticos.

- **Copias de seguridad.** Ante cualquier eventualidad o problema, una copia de seguridad ayudara a recuperar la información.

- **Contraseñas**: Utilizar contraseñas seguras y, lo más recomendable con autenticación de dos pasos.

- **Descarga de software:** El software solo debe descargarse de sitios web oficiales y seguros, nunca a través de enlaces.

- **Sentido común:** Es importante esta recomendación, en caso de duda preguntar a profesionales y entidades especializadas en seguridad informática (Febrero, 2021).

Un sistema de detección de intrusos (IDS)

Un sistema de detección de intrusos (IDS) es hardware y software que emplea firmas de intrusión conocidas para descubrir y analizar el tráfico en la red de entrada y salida para averiguar la actividad anormal.

- Comparan archivos del sistema frente a firmas de malware.
- Procedimientos de escaneo que descubren signos de ataques maliciosos.
- Monitorizar el comportamiento de los usuarios para descubrir intenciones maliciosas.
- Seguimiento de configuraciones y configuraciones que son del sistema.
- Supervisión del tráfico en la red de entrada y salida de dispositivos (Ciberseguridad Industrial by Logitek, 2020).

Sistema de Prevención de Intrusos (IPS)

Un sistema de prevención de intrusiones (IPS) es un programa de seguridad que se permite defender los sistemas de ataques e intrusiones informáticos de manera preventiva. En otras palabras, es un sistema de seguridad proactivo, que realiza monitoreo y análisis en tiempo real en las conexiones y protocolos para así estar pendiente si un ataque está por ocurrir o ha comenzado a ocurrir y proceder a interrumpirlo enviando una alarma a los responsables del sistema de seguridad.

- Bloquea la dirección IP desde la que se origina la amenaza.
- Detiene el proceso, si la actividad maliciosa procede de uno específico.

- Se encarga de suspender o desactivar diversas cuentas de usuario.

- Apaga los sistemas completos para restringir los daños que puedan ocurrir.

- Manda una alerta a los que administran del sistema, registra el incidente y reportar la actividad sospechosa que detecta (Grupo Atico34, 2021).

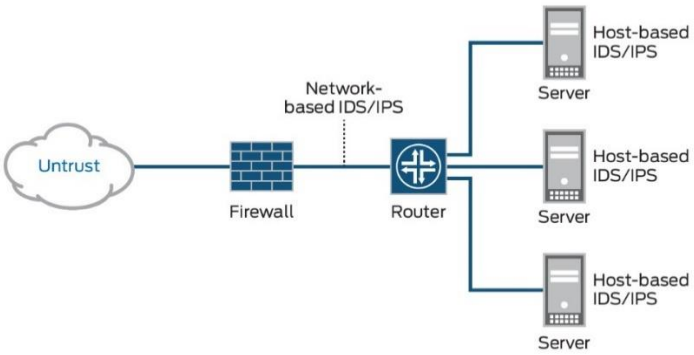


Ilustración 4 ¿Qué son IDS y SPI?
Fuente: https://www.juniper.net/mx/es/research-topics/what-is-ids-ips.html

Amenazas informáticas

Las amenazas informáticas son oportunidades en las que los ciberdelincuentes informáticos logran ingresar a sus computadoras, dispositivos y/o servidores con el propósito de obtener información. Estos ataques, según el tipo, pueden ser a través de correos electrónicos engañosos dando clic en anuncios maliciosos, entre otros.

Las razones principales para que los ciberdelincuentes informáticos ejecutan amenazas cibernéticas son para conseguir información confidencial de sus víctimas colapsando su conexión a Internet a través de ataques informáticos e infectar más computadoras o dañar la Red de Seguridad Perimetral (arroba system, 2021).

DISEÑO DE UNA RED DE SEGURIDAD PERIMETRAL PARA LA UNIVERSIDAD TÉCNICA DE BABAHOYO

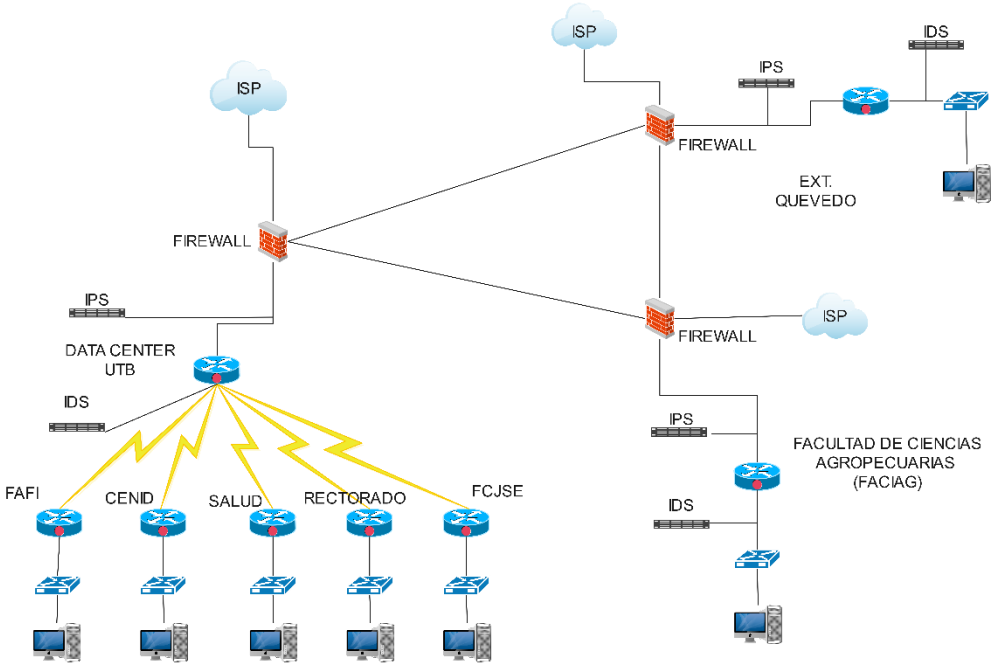


GRÁFICO 1 DISEÑO DE UNA RED PERIMETRAL
Elaborado por: *Fani Yudid Cabrera Vásquez*

Se propone un diseño de una Red de Seguridad Perimetral basada en Open Source para aplicación de IDS e IPS para el control de amenazas informáticas en la Universidad Técnica de Babahoyo; por lo que, esto permite mejorar la Red llegando a tener un nivel muy alto de seguridad, en el cual es muy favorable para la institución con la finalidad de detectar y evitar ataques informáticos a la entidad; por ende, al plantear una virtualización se deja en constancia los resultados obtenidos en esta investigación.

CONCLUSIONES

Al finalizar la presente investigación mediante el respectivo método de investigación se definió las técnicas de recolección de información, la cual el uso de una Red de Seguridad Perimetral basada en Open Source permite mejorar la seguridad y esto ayuda a evitar ataques internos y externos que llegue a tener la institución; por ende, se llega a las siguientes conclusiones:

- Toda red de trabajo de cualquier institución se encuentra constantemente amenazada por ataques informáticos que pueden ocasionar pérdida de información, por lo tanto, es necesario proteger la información a través de políticas de seguridad aplicadas a la red y aunque no se cuente con los recursos necesarios se logró diseñar una Red de Seguridad Perimetral basada en Open Source que permita detectar y notificar las amenazas informáticas por el administrador, garantizando la seguridad de la información.

- La utilización de un firewall brinda protección a la red; a pesar de ello, no asegura la seguridad de todo la Red Perimetral, por tal razón es necesario combinar diferentes elementos de seguridad que ayuden a proteger la información de posibles ataques informáticos.

- Tras finalizar el presente documento se concluyó que la Seguridad Informática es fundamental para las redes de datos de hoy en día, debido al enorme crecimiento de las comunicaciones globales. El sistema de seguridad perimetral apoya a los administradores de Red a cuidar la información que recorre por la red corporativa de una forma más eficaz, gracias a la unión de diversas funcionalidades como el Firewall, IDS e IPS.

BIBLIOGRAFÍA

arroba system. (4 de Febrero de 2021). arroba system. Obtenido de https://arrobasystem.com/blogs/blog/que-son-las-amenazas-informaticas-y-como-protegerte-de-ellas

Ciberseguridad Industrial by Logitek. (8 de Julio de 2020). Industrial Cibersecurity by Logitek . Obtenido de https://www.ciberseguridadlogitek.com/ids-vs-ips-cual-es-la-diferencia/

ciberseguridad México, Fortinet México, seguridad de redes México. (29 de Noviembre de 2021). Ti America. Obtenido de https://www.ti-america.com/en-que-consiste-la-seguridad-perimetral/

EQUIPO COREMAIN. (1 de Octubre de 2021). COREMAIN. Obtenido de COREMAIN: https://www.coremain.com/open-source-ventajas-y-riesgos/

Febrero, A. (14 de Septiembre de 2021). SEGURILATAM. Obtenido de SEGURILATAM: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/software-libre-ventajas-y-vulnerabilidades_20210914.html

Fernández, L. (7 de Marzo de 2020). RZredeszone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/segmentacion-red-vlan-que-es/

Fernández, L. (19 de Abril de 2022). RZredeszone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/mejores-firewall-open-source-proteger-red/

Grupo Atico34. (29 de Septiembre de 2021). Atico34. Obtenido de https://protecciondatos-lopd.com/empresas/sistema-prevencion-intrusiones-ips/

Grupo Atico34. (19 de Febrero de 2021). Grupo Atico34. Obtenido de https://protecciondatos-lopd.com/empresas/seguridad-perimetral-informatica/

Hubbard, B. (25 de Julio de 2022). Invgate. Obtenido de https://blog.invgate.com/es/seguridad-perimetral-informatica

Imagar Solutions Company. (17 de Noviembre de 2020). Imagar Solutions Company. Obtenido de https://www.imagar.com/blog-desarrollo-web/seguridad-perimetral-que-supone/

INGENIERÍA Y TECNOLOGÍA. (30 de Julio de 2020). UNIR LA UNIVERSIDAD EN INTERNET. Obtenido de https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

Morales, F., Toapanta, S., & Toasa, R. M. (11 de Diciembre de 2019). ResearchGate. Obtenido de https://www.researchgate.net/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion

Perez Padilla, J. (22 de Octubre de 2020). CCOSS. Obtenido de CCOSS: https://ccoss.org/slides/CCOSS-Seguridad%20en%20Open%20Source-Javier%20Perez.pdf

Puente, L. (2 de Marzo de 2018). SI-MAD. Obtenido de SI-MAD: http://www.si-mad.com/como-gestionar-la-seguridad-perimetral-de-tu-empresa/

USS Seguridad Integral. (21 de Octubre de 2021). USS. Obtenido de https://uss.com.ar/consejos-uss/mejorar-la-seguridad-perimetral-de-una-empresa/

Villalta, L. (5 de Mayo de 2018). NANOPDF. Obtenido de https://nanopdf.com/download/elementos-basicos-de-la-seguridad-perimetral_pdf#

ANEXOS

Entrevista

Preguntas a Ingenieros

1- **¿Por qué es importante la seguridad de la red de una organización?**
   Referencia: Anexo Pregunta 1

El Ing. Andrés Alfonso Martínez Campoverde manifestó que, el valor de la estabilidad informática de las organizaciones radica en esencia en que la implementación maliciosa de sus sistemas de información privados y de los recursos internos puede acarrear desastrosas secuelas en cada una de las superficies de la organización, deviniendo en inconvenientes tanto productivos como financieros.

El Ing. Aron Jimmy Diaz Meneses comentó que, la pérdida de datos, la realidad de malintencionados virus, la intromisión de desaprensivos o, sencillamente, el inadecuado ingreso e implementación de nuestra red o nuestras propias comunicaciones, tienen la posibilidad de y acostumbran a situar en serio riesgo la buena marcha de nuestra compañía.

El Ing. Carlos Alejandro Coello Castro mencionó que, ningún cliente confiaría en sus datos, su información personal y confidencial a una empresa con problemas de seguridad, arriesgando la pérdida de las mismas. Por eso se ha vuelto fundamental que las organizaciones implementen una red segura y así brindar un servicio confiable a los usuarios.

2- **¿Una red perimetral mejora la seguridad de la red de una organización? ¿Por qué?**

Referencia: Anexo Pregunta 2

El Ing. Andrés Alfonso Martínez Campoverde manifestó que, porque están compuestos por sistemas y equipos eléctricos y mecánicos integrados que protegen el perímetro exterior de una propiedad que queremos mantener segura. Su objetivo principal es detectar intrusos porque protege la empresa a nivel operativo y físico.

El Ing. Aron Jimmy Diaz Meneses comentó que, mientras la tecnología avanza, los piratas informáticos se tornan más hábiles y sofisticados en sus técnicas de ataque. Los administradores tienen que estar al tanto de las últimas amenazas y tener una estrategia para defender sus redes, y una de las superiores formas de defender la red es aplicando una red perimetral. Porque se utiliza para controlar el tráfico entrante y saliente, así como para proteger la red de ataques externos.

- Protege la empresa contra ataques externos
- Detección de intrusiones

El Ing. Carlos Alejandro Coello Castro mencionó que, mejora la seguridad, ya que establece una barrera que previene ataques que pueden infectar la red, actuando como un filtro, permite el tráfico entre la organización y el exterior, pero bloquea el tráfico malicioso.

3- ¿Qué beneficios tiene una red perimetral basada en open source?

Referencia: Anexo Pregunta 3

El Ing. Andrés Alfonso Martínez Campoverde manifestó que, el beneficio de comprobar y permitir/denegar tanto el tráfico entrante o saliente disminuir los ataques de seguridad informática ya sean ataques DoS para intentar dejar inutilizado un servidor web, e incluso ataques para infectarnos con programa maligno.

El Ing. Aron Jimmy Diaz Meneses comentó que, el beneficio de disminuir los incidentes de seguridad informática, la búsqueda se realizó en bases de datos como I-explore, Google Academic, Web of Science y Tandfonline para ampliar el tema de investigación.

El Ing. Carlos Alejandro Coello Castro mencionó que, los beneficios son los siguientes:

- Previene problemas de seguridad y ataques maliciosos.
- Brinda mayor seguridad y confiabilidad.

4- **¿Contra qué tipos de ataques informáticos protege una red perimetral a una institución?**

Referencia: Anexo Pregunta 4

El Ing. Andrés Alfonso Martínez Campoverde manifestó que:

- Denegar el tráfico de red.
- Funciones de routing y firewall avanzadas
- Libre entrada a ataque malicioso

El Ing. Aron Jimmy Diaz Meneses comentó que:

- Un excesivo consumo de ancho de banda
- Inadecuada utilización de los servicios de red
- Libre entrada de virus malicioso

El Ing. Carlos Alejandro Coello Castro mencionó que, protege contra los ataques de intrusión de la red y también de ataques que provocan la negación del servicio.

5- **¿Qué ventajas tiene IDS e IPS en la red de una institución?**

Referencia: Anexo Pregunta 5

El Ing. Andrés Alfonso Martínez Campoverde manifestó que, la principal ventaja de un sistema IDS y IPS es la capacidad de detectar ataques cibernéticos, además de realizar acciones que logran anular sus efectos y la protección está enfocada en un sólo

usuario o un reducido grupo.

El Ing. Aron Jimmy Diaz Meneses comentó que, la principal ventaja de un sistema IDS y IPS es que permite ver lo que está sucediendo en la red en tiempo real en base a la información recopilada, reconocer modificaciones en los documentos y automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red.

El Ing. Carlos Alejandro Coello Castro mencionó que, una de las ventajas de los IDS e IPS es que sirven para monitorizar el tráfico que entra y sale de la red de la organización.

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, 14 de julio de 2022
D-FAFI-UTB-0279-2022

DECANO FAFI
Agradecere proceder con el trámite de ley que corresponde
Ing. Marcos Oviedo Ph. D
RECTOR UTB
25/07/2022

Ingeniero
Marcos Oviedo Rodríguez, Ph.D.
RECTOR
UNIVERSIDAD TÉCNICA DE BABAHOYO.
En su Despacho. –

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

la Señorita **CABARERA VASQUEZ FANI YUDID,** con cédula de identidad No. 095358441-4, Estudiante de la Carrera de Ingeniería en Sistemas, matriculada en el proceso de titulación en el periodo Abril 2022 – Septiembre 2022, trabajo de titulación modalidad Caso de Estudio, previo a la obtención del grado académico profesional universitario de tercer nivel como **INGENIERA EN SISTEMAS,** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Caso de Estudio en la institución de su digna Rectoría, el cual titula: **DISEÑO DE UNA RED DE SEGURIDAD PERIMETRAL BASADA EN OPEN SOURCE PARA APLICACIÓN DE IDS E IPS PARA EL CONTROL DE AMENAZAS INFORMATICAS EN LA UNIVERSIDAD TÉCNICA DE BABAHOYO.**

Del señor Rector,

Atentamente.

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO

C/c: Archivo

RECIBIDO
UNIVERSIDAD TECNICA DE BABAHOYO
SECRETARIA FAFI
25/07/2022 HORA:

RECIBIDO
21/07/2022 16:01
19

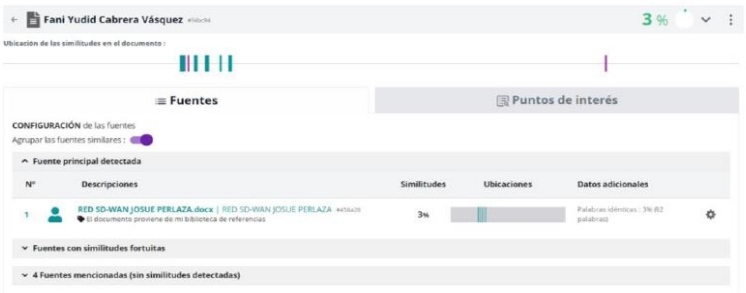
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA EN SISTEMAS

Babahoyo 11 de Agosto del 2022

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: el/la, Sr./Sra./ Srta.: Fani Yudid Cabrera Vasquez, cuyo tema es: DISEÑO DE UNA RED DE SEGURIDAD PERIMETRAL BASADA EN OPEN SOURCE PARA APLICACIÓN DE IDS E IPS PARA EL CONTROL DE AMENAZAS INFORMATICAS EN LA UNIVERSIDAD TECNICA DE BABAHOYO, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[3 %]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Firmado electrónicamente por:
IVAN RUBEN RUIZ

Ing. Sist. Iván Rubén Ruiz Parrales, Msg
DOCENTE DE LA FAFI.