UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO 2023 – OCTUBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

EVALUACION DE LA SEGURIDAD INFORMATICA EN LA UNIVERSIDAD TECNICA DE BABAHOYO MEDIANTE EL ANALISIS DE TRAFICO INTEGRAL EN REDES DE AREA LOCAL

ESTUDIANTE:

CASTRO ROMAN ANGIE SCARLETTE

TUTOR:

MONTECE MORENO OMAR RODRIGO

AÑO 2023

Contenido

RESUMEN

Este estudio se centra en evaluar la seguridad informática en la Universidad Técnica de Babahoyo, con un enfoque en su red de área local (LAN). Se analizan las políticas de seguridad implementadas, las amenazas cibernéticas enfrentadas y las medidas de seguridad adoptadas. Además, se realiza un análisis de tráfico de red para identificar posibles riesgos. Se discuten incidentes de seguridad pasados y amenazas actuales, como ataques de malware y escaneos de puertos.

Las medidas de seguridad, como el uso de un firewall Fortinet y un sistema de detección de intrusiones, se describen de manera resumida. Se mencionan recomendaciones para mejorar la seguridad, como la actualización de sistemas. La ausencia de una estrategia integral de seguridad informática y de políticas claras de protección de datos y privacidad puede dejar expuestos los sistemas y la información sensible de la universidad a posibles ataques y explotación por parte de actores malintencionados.

Palabras clave: seguridad informática, redes de área local (LAN), políticas de seguridad, amenazas cibernéticas, análisis de tráfico

ABSTRACT

This study focuses on assessing computer security at the Technical University of Babahoyo, with a focus on its local area network (LAN). The security policies implemented, the cyber threats faced and the security measures adopted are analysed. In addition, a network traffic analysis is conducted to identify potential risks. Past security incidents and current threats, such as malware attacks and port scans, are discussed.

Security measures, such as the use of a Fortinet firewall and an intrusion detection system, are summarised. Recommendations for improving security, such as upgrading systems, are mentioned. The absence of a comprehensive IT security strategy and clear data protection and privacy policies may leave the university's systems and sensitive information exposed to possible attacks and exploitation by malicious actors.

Keywords: computer security, local area networks (LANs), security policies, cyber threats, traffic analysis

PLANTEAMIENTO DEL PROBLEMA

Debido al creciente uso de las tecnologías de la información y la comunicación en las instituciones educativas, la seguridad informática de las redes de área local se ha convertido en un verdadero desafío. Aunque la digitalización de los procesos y servicios otorga muchos beneficios, también implica la exposición a amenazas cibernéticas, ataques de hackers y filtraciones de datos. La falta de una adecuada atención y enfoque en la seguridad informática ha dado lugar a diversos riesgos y vulnerabilidades que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas y datos institucionales. La integridad y el funcionamiento eficiente de los recursos informáticos de la universidad dependen en gran parte de la protección de los datos sensibles y la privacidad de los usuarios.

La problemática radica en distintos aspectos como la falta de comprensión y conciencia sobre los riesgos de seguridad informática que enfrentan las redes de área local de la Universidad Técnica de Babahoyo, así como la falta de medidas efectivas para prevenir y mitigar estos riesgos. Esto puede llevar a prácticas inseguras como la apertura de correos electrónicos o enlaces sospechosos, y la descarga de archivos o software no confiables, además de una subestimación de los riesgos y falta de sentido de urgencia en la implementación de medidas de seguridad. La ausencia de una estrategia integral de seguridad informática y de políticas claras de protección de datos y privacidad puede dejar expuestos los sistemas y la información sensible de la universidad a posibles ataques y explotación por parte de actores malintencionados.

La proliferación de dispositivos móviles y la práctica de BYOD (*Bring Your Own Device*) en el entorno universitario generan un desafío adicional en términos de seguridad informática. El uso de dispositivos personales y su conexión a las redes de

área local pueden aumentar la superficie de ataque y dificultar el control y la protección de los datos y sistemas institucionales. Sin embargo, esta tendencia también introduce nuevos riesgos de seguridad, ya que estos dispositivos pueden ser más vulnerables a ataques y pueden ser utilizados como vectores de entrada a la red de área local.

Las amenazas de malware, como virus, ransomware y troyanos representan una preocupación constante en el entorno universitario. La falta de conocimiento y concienciación entre los usuarios puede conducir a la caída en trampas de phishing y a la instalación de malware, lo que puede causar daños graves, como la pérdida o el cifrado de datos, así como interrupciones en los servicios críticos.

La insuficiente capacitación y formación en seguridad informática del personal encargado de la gestión de las redes de área local de la institución, representa un desafío significativo para la protección de los sistemas y los datos institucionales. La falta de conocimiento actualizado sobre las últimas amenazas y técnicas de protección crea una brecha en la capacidad del personal para implementar y mantener medidas de seguridad adecuadas. Esto puede llevar a la existencia de configuraciones inseguras, falta de actualizaciones de software, contraseñas débiles y una comprensión limitada de las mejores prácticas en seguridad informáticas.

La investigación se centra en los riesgos de seguridad informática presente en las redes de área local de la Universidad Técnica de Babahoyo, incluyendo la vulnerabilidad a ciberataques, fugas de datos, acceso no autorizado a recursos de la red y el cumplimiento normativo legal. La identificación y comprensión de estor riesgos es crucial para implementar medidas adecuadas de seguridad y proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos de la universidad.

JUSTIFICACION

La creciente amenaza de los ataques cibernéticos y la necesidad de proteger los sistemas y datos institucionales ha hecho que sea de vital importancia la realización de un estudio sobre los riesgos de seguridad informática mediante el análisis de tráfico en las redes de área local de la Universidad Técnica de Babahoyo. La institución almacena y maneja gran cantidad de datos confidenciales, como información estudiantil, investigaciones académicas y documentos administrativos. Esto también implica la información personal y financiera de los miembros de la comunidad universitaria.

La interrupción de los servicios y sistemas informáticos pueden tener un impacto significativo en la operatividad de la universidad. Un ataque cibernético exitoso puede resultar en la paralización de las actividades académicas y administrativas, la pérdida de información crítica y la interrupción de la comunicación interna y externa. La comprensión y mitigación de los riesgos de seguridad informática ayudará a salvaguardar la continuidad operativa de la institución, garantizando que los servicios y sistemas se mantengan disponibles y funcionales.

La realización de esta investigación proporcionará una valiosa oportunidad de generar conciencia y educar a la comunidad universitaria sobre los riesgos de seguridad informática y la importancia de las mejores prácticas de seguridad. El análisis de tráfico promoverá la cultura de protección y seguridad en toda la comunidad universitaria. Los involucrados comprenderán mejor la importancia de mantener sus dispositivos y contraseñas seguras, evitar prácticas riesgosas como hacer clic en enlaces desconocidos, compartir información confidencial, entre otros.

OBJETIVOS

OBJETIVO GENERAL

- Evaluar la seguridad informática mediante el análisis de tráfico en las redes de área local de la Universidad Técnica de Babahoyo, identificando las vulnerabilidades existentes y proponiendo medidas de protección efectivas.

OBJETIVOS ESPECIFICOS

- Analizar el tráfico en las redes de área local de la Universidad Técnica de Babahoyo mediante herramientas especializadas para identificar patrones de comportamiento y posibles anomalías.
- Evaluar los riesgos de seguridad informática asociados con los patrones de tráfico identificados, priorizándolos según su impacto potencial en la confidencialidad, integridad y disponibilidad de los sistemas e información institucional.
- Proponer recomendaciones y medidas de mitigación específicas para abordar los riesgos identificados y fortalecer la seguridad informática de la universidad.

LÍNEAS DE INVESTIGACIÓN

La presente investigación está orientada con la línea de investigación "Sistemas de información y comunicación, emprendimiento e innovación". Esta línea de investigación se relaciona directamente con el caso de estudio sobre seguridad informática en las redes de área local en la Universidad Técnica de Babahoyo, ya que ambas comparten la búsqueda de soluciones tecnológicas avanzadas y el impulso de la innovación en el ámbito de la seguridad informática.

La sublínea de investigación denominada "Redes y tecnologías inteligentes de software y hardware", también tiene una clara relación con el estudio de caso, ya que implica el estudio minucioso del flujo de datos y la interacción entre dispositivos, lo que permite identificar patrones de comportamiento, tendencias y posibles vulnerabilidades. El enfoque en tecnologías inteligentes también sugiere la aplicación de técnicas de aprendizaje automático y análisis predictivo para mejorar la detección de amenazas y la toma de decisiones en materia de seguridad informática.

La línea y sublínea de investigación establecen un marco teórico y conceptual idóneo para el estudio de caso sobre la seguridad informática en las redes de área local de la Universidad Técnica de Babahoyo. Estos enfoques multidisciplinarios y tecnológicos permitirán una evaluación detallada de los riesgos, una propuesta de soluciones innovadoras y una contribución significativa al fortalecimiento de la protección de los sistemas e información institucional.

ARTICULACION DEL TEMA

Durante el período de prácticas preprofesionales se desarrollaron una serie de actividades relacionadas con la tecnología y la gestión de redes. Una de las responsabilidades clave fue la configuración y el mantenimiento de la red de área local (LAN) de una bodega de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo.

Durante este proceso, surgió una creciente preocupación por la seguridad de la red y la integridad de los datos que transitaban por ella. Esta experiencia llevó a considerar la importancia crítica de la seguridad informática en un entorno académico y a plantear cuestiones sobre cómo evaluar y mejorar la seguridad en las redes LAN universitarias.

La articulación del presente tema de investigación tiene como objetivo principal desarrollar un enfoque sólido para evaluar la seguridad informática en las redes LAN académicas y, en particular, en la Universidad Técnica de Babahoyo. Los resultados de la investigación se utilizarán con el objetivo de determinar el nivel de seguridad de la red y proponer recomendaciones destinadas a fortalecer la seguridad de la misma.

MARCO CONCEPTUAL

Políticas de seguridad

Las políticas de seguridad son directrices y procedimientos que respaldan la seguridad de acuerdo con los requisitos legales y de negocio. La implementación de la política de seguridad implica el uso de metodologías que establecen restricciones sobre las acciones permitidas y no permitidas, con el objetivo de establecer mecanismos que prevengan y detecten intrusiones, así como permitan la recuperación de los sistemas o redes. (Postigo Palacios, 2020)

Siguiendo esta línea, las políticas de seguridad son esenciales para proteger la integridad de la información. Sirven como pautas y estrategias para garantizar que los requisitos legales y empresariales se cumplan.

Amenaza

De acuerdo con (Irwin, 2020) una amenaza se define como cualquier incidente, sea intencional o accidental, que pueda tener un impacto negativo en un activo, incluyendo su pérdida, desconexión o acceso no autorizado. Estas amenazas podrían comprometer la confidencialidad, integridad o disponibilidad de un activo.

En cuanto a las redes, una amenaza implica cualquier intento de violar la red y acceder a los sistemas de datos, representando así un riesgo para la integridad de la red y la protección de la información. Existen diversos tipos de amenazas de red, cada una con objetivos distintos. Por ejemplo, los ataques de denegación de servicio (DDoS) tienen la intención de inundar la red o los servidores con solicitudes para provocar su inoperatividad. Otras amenazas, como el malware o el robo de credenciales, buscan obtener acceso no autorizado a los datos. (SecurityScorecard, 2021)

En resumen, una amenaza abarca un incidente, intencionado o no que pueda

generar efectos negativos en activos, lo que podría involucrar pérdida, daño o modificaciones no autorizados.

Amenaza informática

En línea con lo que sostiene (Hernandez, 2022), una amenaza informática consiste en la utilización de debilidades o errores en un sistema, con la finalidad de comprometer su funcionamiento, y así obtener beneficios en el proceso.

Estas amenazas pueden ser categorizadas en dos grupos principales en función de su origen

Externas. Estas amenazas provienen de fuentes externas a la organización y están fuera del control directo del departamento de Tecnología de Información.

Internas. Se originan dentro de la propia organización y están, en cierta medida, bajo el alcance de control del departamento de TI.

Según (Casetto, 2023) los principales tipos de amenazas a la seguridad informática son:

Ataques de malware

Los ataques emplean diversas técnicas para infiltrar malware en los dispositivos de los usuarios, a menudo a través de engaños o vulnerabilidades. Una vez instalado, el malware puede vigilar actividades, robar datos y permitir al atacante controlar el dispositivo o usarlo con fines maliciosos. Entre ellos se encuentran los troyanos, ransomware, spyware, gusanos, entre otros.

Ataques de ingeniería social

Consisten en manipular de manera psicológica a los usuarios incitándolos a realizar acciones beneficiosas para el atacante o divulgar información sensible. Entre los ataques más comunes de ingeniería social están:

Ataques a la Cadena de Suministro de Software

Implica un ciberataque hacia una organización con el propósito de explotar puntos débiles en su confiable cadena de suministro y actualización de software. Dicha cadena representa la interconexión de individuos, entidades, recursos, actividades y tecnologías involucradas en la fabricación y comercialización de un producto. Estos ataques se enfocan en explotar la confianza que las organizaciones depositan en sus proveedores externos, especialmente en lo que respecta a actualizaciones y correcciones.

Amenazas Persistentes Avanzadas (APT)

Cuando un individuo o grupo accede de manera no autorizada a una red y permanece sin detección durante un extenso período, los atacantes pueden extraer información confidencial mientras evitan ser identificados por el personal de seguridad. Ya que requieren de grandes habilidades, por lo general, se dirigen a estados, grandes corporaciones u otros objetivos de gran valía.

Denegación de servicio distribuida (DDoS)

Busca abrumar los recursos de un sistema específico, provocando su inoperancia y bloqueando el acceso a sus usuarios. Esta variante de DoS involucra a los atacantes que comprometen numerosos dispositivos, como computadoras, y los coordinan en un asalto conjunto contra el objetivo.

Ataques Man-in-the-Middle (MitM)

Cuando usuarios o dispositivos establecen conexión con un sistema remoto vía Internet, asumen que se comunican de manera directa con el servidor del sistema al que intentan acceder. No obstante, en un ataque MitM, los atacantes desafían esta percepción al posicionarse entre el usuario y el servidor de destino. Una vez que el atacante ha interceptado la comunicación, podría tener la capacidad de comprometer las credenciales del usuario, sustraer datos delicados y presentar respuestas distintas al

usuario.

Ataques a credenciales

Un ciberdelincuente puede obtener información de contraseñas de un individuo mediante el monitoreo de la conexión a la red, empleando tácticas de ingeniería social, realizando intentos de adivinanza (de manera aleatoria o sistemática) o accediendo a bases de datos de contraseña.

Desde mi perspectiva, una amenaza informática se encarga de explotar debilidades en sistemas para obtener ventajas y dañar el funcionamiento. Estas se dividen en externas e internas, y hay de distintos tipos. Los tipos comunes de amenazas como malware e ingeniería social hacen pensar en que el eslabón más débil en los sistemas y redes son las personas.

Activo

Un Activo se define como cualquier elemento, dato o dispositivo presente en los sistemas de una organización que posee valor, especialmente debido a su contenido de información sensible o a su capacidad para acceder a dicha información.

Entre los activos más comunes de una organización se encuentran los activos de información, los cuales incluyen bases de datos y archivos físicos que contienen datos sensibles y confidenciales. (Irwin, 2020)

En línea con la definición propuesta por Irwin, un activo se define como cualquier componente tangible o intangible en los sistemas de una organización que posee valor.

Protección de datos

La protección de datos se refiere a los derechos que tienen los individuos cuyos

datos son adquiridos, conservados a y procesados, de estar al tanto de qué información está siendo retenida y utilizada, y de rectificar cualquier inexactitud. (CEPAL, 2020)

Analizando la investigación de CEPAL se puede concluir que la protección de los datos implica que las personas tienen derecho a saber qué información suya está siendo utilizada y con qué propósito, además de que su información o datos no puede ser divulgada sin su consentimiento.

Vulnerabilidad

Una vulnerabilidad se define como una debilidad o defecto dentro de la organización que puede ser explotado por una amenaza, poniendo en riesgo, dañando o destruyendo un activo.

Es común encontrar vulnerabilidades en los programas informáticos debido a su complejidad y a las frecuentes actualizaciones que reciben. No obstante, también puede manifestarse como puntos débiles físicos, como una cerradura rota que permita a personas no autorizadas acceder a áreas restringidas de las instalaciones, o incluso como proceso procesos mal diseñados o inexistentes que podrían llevar a los empleados a exponer información confidencial. (Irwin, 2020)

En retrospectiva, una vulnerabilidad se refiere a un aspecto interno en una organización que puede ser aprovechada por amenazas, para causar daño. Estas pueden ser tanto lógica como físicas.

Redes de Área Local (LAN)

Según (Corao & Vanegas, 2023) a red de área local o red LAN es un tipo de red

que se ubica en un área geográfica específica y que no abarca grandes distancias. De hecho, una red LAN se limita a espacios de trabajo restringidos, como una casa, una oficina, un departamento en una oficina corporativa o edificio de trabajo, etc. (pág. 5)

Topologías de red

Se refiere a la disposición estructural y la forma en que los dispositivos y nodos de una red de área local (LAN), están interconectados. Define cómo se conectan los dispositivos, cómo se transmiten los daros y cómo se comunican entre sí. La elección de la topología afecta en la eficiencia, la redundancia y la confiabilidad de la red. Según (Escudero et al., 2022) las topologías comunes son:

Topología en bus: Todos los dispositivos se enlazan mediante un único canal central denominado bus. Para establecer esta conexión, se emplea un cable coaxial, lo cual requiere que la tarjeta de red cuente con un conector BN para vincularse al bus.

Topología en anillo: Cada dispositivo se enlaza con los dos nodos vecinos para crear una configuración en forma de anillo. Se requiere que los dispositivos cuenten con dos tarjetas de red, una para cada conexión. La información fluye en una única dirección, y un solo nodo tiene el permiso para transmitir, controlado por un token o testigo.

Topología en estrella: Es la topología más usada en LAN. Todos los dispositivos se conectan a un nodo central, que actúa como distribuidor, conmutador y controlador del flujo de datos. Este nodo suele ser un switch.

Topología en árbol: Esta estructura se puede concebir como una serie de redes en estrella interconectadas a través de un bus. Un nodo principal, a menudo un enrutador o switch, origina ramificaciones que se conectan a nodos secundarios.

Topología en malla: Cada dispositivo se vincula con uno o más dispositivos de la red. Requiere que cada dispositivo tenga tantas tarjetas de red como conexiones con

otros dispositivos. (pág. 91)

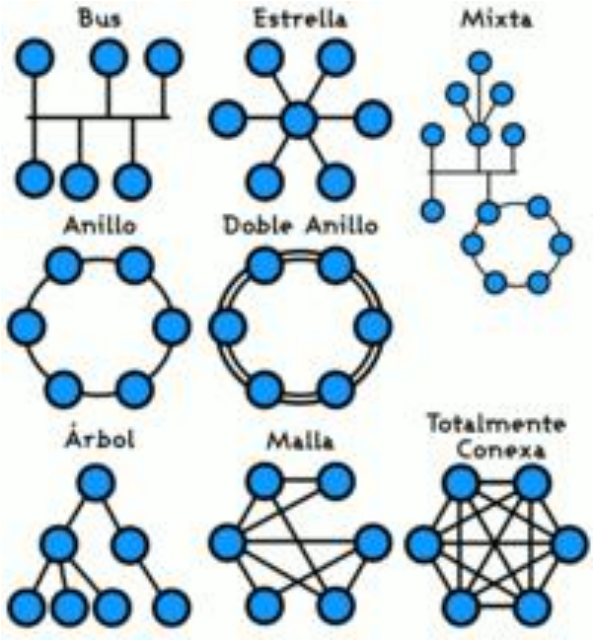


Ilustración 1. Fuente: https://upload.wikimedia.org/wikipedia/commons/thumb/4/4a/Topolog%C3%ADa_de_red.png/200px-Topolog%C3%ADa_de_red.png

De acuerdo con lo mencionado por los autores, una Red de Área Local (LAN) es una red de comunicación confinada a espacios reducidos, como edificios, donde los dispositivos comparten un medio de transmisión para enviar datos a alta velocidad. En cuanto a las topologías de red, se refieren a la estructura de interconexión de dispositivos. Las topologías más comunes son la de bus (conexión en línea), la de anillo (conexión en círculo) y la de estrella (conexión centralizada). Otras variantes incluyen la topología en árbol y en malla, con cada dispositivo vinculado a otros de la red.

BYOD (Bring Your Own Device)

Este término se refiere a la práctica de emplear dispositivos móviles propios del usuario para acceder a la información y sistemas de la empresa en la que este desempeña su labor. La expresión BYOD surgió inicialmente en 2009 como resultado de una iniciativa interna de los empleados de Intel, quienes llevaban sus propios dispositivos a la compañía y los conectaban a la red empresarial. (Hino et al., 2019)

En otras palabras, BYOD (*Bring Your Own Device*) se refiere a la práctica de usar dispositivos personales, como teléfonos o computadoras, para acceder a la información y sistemas de una empresa.

Seguridad informática

Según (Coppola, 2023) la seguridad informática es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado.

La seguridad informática implica establecer normas y técnicas para garantizar la seguridad y disponibilidad de la información. Su objetivo principal es minimizar riesgos provenientes de diversas fuentes, como entrada de datos, hardware y usuarios.

De acuerdo con (Postigo Palacios, 2020) existe la seguridad activa y la seguridad pasiva.

Seguridad activa: Son aquellas medidas que se ejecutan diariamente para evitar cualquier ataque. Están relacionadas con la seguridad lógica.

Seguridad pasiva: Son aquellas medidas correctivas y que mitigan los efectos causados por una amenaza. Estas se realizan después de una amenaza y están relacionadas con la seguridad física. (pág. 12)

Confidencialidad

Se centra en tomar medidas para evitar que información confidencial sea accesible por individuos no autorizados. Es fundamental permitir el acceso de las personas adecuadas a la información, al mismo tiempo que se limita el acceso a aquellos

sin autorización. (OnTek, 2019)

En concordancia con las conclusiones de OnTek, la confidencialidad se refiere a la cualidad de mantener la información en secreto y restringida al acceso de personas no autorizadas.

Integridad

Se enfoca en mantener la coherencia, exactitud y confianza de los datos a lo largo de su ciclo de vida. Durante la transferencia, los datos no deben sufrir modificaciones, y es fundamental implementar medidas para evitar alteraciones no autorizadas, como podría ocurrir en casos de infracciones de confidencialidad. (OnTek, 2019)

Se puede decir que es la garantía de que la información y los datos no han sido alterados de manera no autorizada ni accidental.

Disponibilidad

La disponibilidad implica acceder a la información sin dificultades ni interrupciones cuando se requiere. Si la disponibilidad se ve comprometida, ciertas tareas no podrán realizarse e incluso podría haber una interrupción completa de la actividad o servicio. (Grupo Atico34, 2023)

De acuerdo a lo descrito anteriormente, la disponibilidad es la capacidad de acceder a la información y a los sistemas cuando se necesiten y por quienes lo necesiten, evitando así interrupciones no planificadas y garantizando la continuidad del servicio.

Tráfico de red

Según (Sangfor Technologies, 2022) implica la transferencia de información a través de una red. Distintas actividades y conductas generan diversos tipos de patrones de tráfico en la red. Se pueden distinguir varias categorías para clasificar estos patrones de tráfico.

- Tráfico intenso.
- Tráfico interactivo.
- Tráfico en tiempo no real.
- Tráfico sensible a la latencia.

En línea con lo mencionado, el tráfico de red puede incluir diversos tipos de actividades y patrones de comunicación, como la transmisión de archivos, el intercambio de mensajes y la navegación por Internet. El tráfico de red varía en función de la cantidad de datos que se envían y reciben, así como la naturaleza de las interacciones entre los dispositivos en la red.

Análisis de tráfico de red

El análisis de tráfico de red es un método de inspección y desglose de los paquetes de información que componen el flujo de datos en una red. Este proceso utiliza una combinación de modelado de comportamiento, detección basada en reglas y aprendizaje automático para eliminar cualquier actividad sospechosa. Mediante este análisis, es posible establecer un patrón normal de comportamiento e identificar cualquier actividad inusual como una posible amenaza. Este tipo de análisis se aplica principalmente en la seguridad, pero también puede resultar útil para planificar la capacidad de la red y detectar aumentos repentinos en la actividad en áreas específicas. (Sangfor Technologies, 2022)

El análisis de tráfico de red implica examinar y comprender el flujo de datos y la comunicación entre dispositivos en una red. Esta actividad se realiza para identificar patrones de uso, identificar problemas de rendimiento, detectar posibles amenazas de seguridad y tomar decisiones informadas sobre la optimización de la red. El análisis de tráfico de red implica observar el volumen de datos, los protocolos utilizados, los destinos y orígenes de la comunicación, así como la calidad y eficiencia de la transferencia de datos. Esta información ayuda a los administradores de red a tomar medidas para mejorar la velocidad, la seguridad y la disponibilidad de la red.

Análisis de riesgo

De acuerdo a (Rausand & Haugen, 2020) el análisis de riesgos es un proceso metódico que busca reconocer y explicar posibles situaciones adversas, así como sus orígenes, probabilidades y resultados. Su objetivo principal radica en abordar las tres interrogantes que contribuyen a delinear el concepto de riesgo. (pág. 59)

Tomando en cuenta las observaciones de los autores existen tres aspectos fundamentales a tener en cuenta en el proceso de análisis de riesgo que son identificar las amenazas potenciales, evaluar la probabilidad de que ocurran y medir el impacto que tendrían en los objetivos. Mediante este proceso, se determina la importancia de cada riesgo y se toman decisiones informadas sobre cómo mitigarlos o abordarlos.

Firewall

Según (Cep, 2019) un cortafuegos o *firewall* es una componente dentro de un sistema o red diseñado con el propósito de bloquear accesos no autorizados, al mismo tiempo que permite comunicaciones permitidas. Esencialmente, consiste en un conjunto de dispositivos configurados para regular, mediante criterios y reglas predefinidas, el

tráfico de red, permitiendo o restringiendo, cifrando o descifrando, de acuerdo a políticas establecidas. Este elemento, que puede ser tanto de hardware como de software, supervisa las comunicaciones autorizándolas o bloqueándolas conforme a las políticas de red establecidas por el administrador u organización responsable. (pág. 34)

Basándonos en esa interpretación, podemos definir a un firewall como una barrera de seguridad que se utiliza para proteger una red o sistema informático contra amenazas cibernéticas. Actúa como un filtro entre la red interna y externa, controlando el flujo de datos y permitiendo o bloqueando el acceso según ciertas reglas. El firewall puede prevenir el acceso no autorizado, detectar y bloquear ataques maliciosos, y permitir una gestión más controlada de la comunicación entrante y saliente. Puede ser implementado a nivel de hardware o software y es esencial en la estrategia de seguridad informática de una organización.

MARCO METODOLOGICO

Para la realización de este caso de estudio se empleó una combinación de técnicas y enfoques de investigación para lograr los objetivos de análisis y evaluación de riesgos de seguridad informática en la red de área local de la Universidad Técnica de Babahoyo.

Se llevó a cabo una exhaustiva revisión de literatura y documentación relacionada con la seguridad informática, análisis de tráfico de redes, y metodologías de evaluación de riesgos. Se seleccionaron fuentes confiables y actualizadas para fundamentar el marco teórico y el enfoque metodológico del estudio.

Con el objetivo de recopilar información crucial y detallada sobre la infraestructura de red, sistemas utilizados, políticas de seguridad actuales, incidentes previos y desafíos enfrentados en el ámbito de seguridad informática se realizaron entrevistas al especialista en redes y al director del departamento de sistemas de la Universidad Técnica de Babahoyo.

Para el análisis de tráfico en las redes de la universidad se utilizará el firewall de Fortinet. Mediante la captura y evaluación del tráfico, se identificarán patrones de comportamiento y posibles anomalías que podrían indicar riesgos de seguridad. Utilizando la información recopilada de las entrevistas y los resultados del análisis de tráfico, se identificarán y evaluarán los riesgos de seguridad. Estas propuestas estarán orientadas a mejorar la protección de la red y los sistemas, así como a fortalecer las prácticas de seguridad informática.

RESULTADOS

En esta sección, se presentan los resultados obtenidos a partir del análisis exhaustivo de tráfico en las redes LAN de la Universidad Técnica de Babahoyo. Para efectos de la investigación se tomará en cuenta el consumo de ancho de banda y aplicaciones, el uso web, y las amenazas.

Consumo de Ancho de Banda y Aplicaciones

Los resultados del análisis de consumo de ancho de banda y patrones de aplicaciones en la red de la Universidad Técnica de Babahoyo revelan importantes aspectos en relación a la seguridad informática. Por ejemplo, se observó que el tráfico recibido supera al tráfico enviado, indicando una posible mayor carga de tráfico entrante en comparación con el tráfico saliente. Asimismo, los picos en la cantidad de sesiones en ciertos días, como el 4 y 8 de agosto, sugieren momentos de actividad intensa que podrían indicar actividad anómala o intentos de ataque.

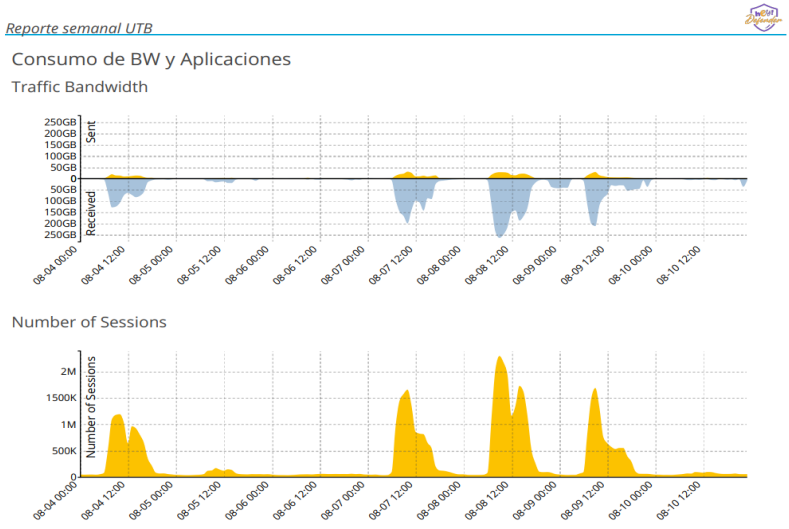


Ilustración 2. Fuente: Departamento de Sistemas - Universidad Técnica de Babahoyo

Uso Web

El análisis del uso de la web en la red reveló patrones de comportamiento interesantes relacionados con las actividades de navegación de los usuarios. Como se observa en las imágenes proporcionadas, se analizaron usuarios con actividad inusualmente alta, así como el consumo de ancho de banda por parte de usuarios y categorías específicas. También se investigaron actividades de correo electrónico, considerando tanto el número como el tamaño de los correos electrónicos enviados y recibidos.

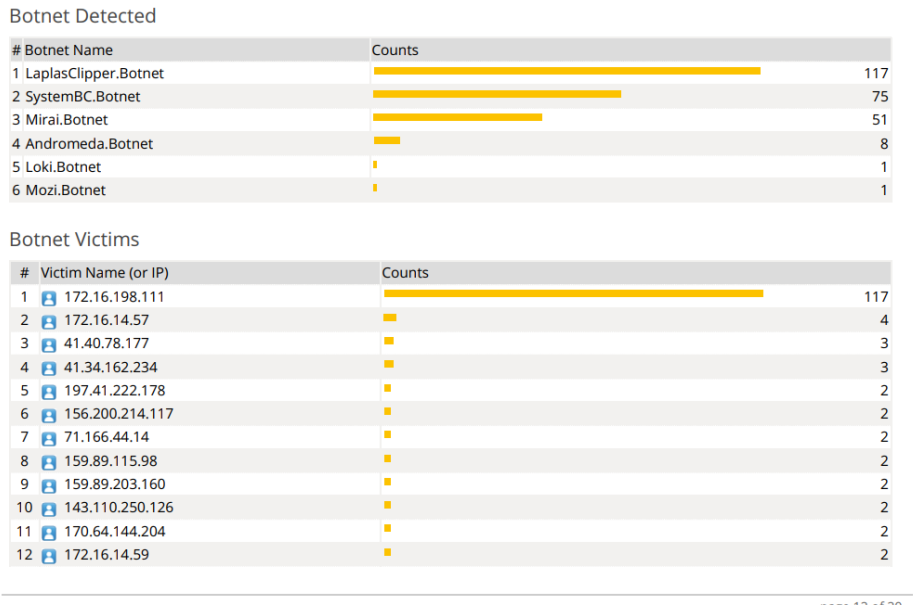
Top 20 Most Active Users

#	User (or IP)	Hostname	Requests
1	172.16.2.20	172.16.2.20	121,371
2	172.16.22.54	172.16.22.54	108,824
3	172.16.7.51	172.16.7.51	89,977
4	172.16.22.56	172.16.22.56	84,131
5	172.16.13.51	172.16.13.51	82,512
6	172.16.7.71	172.16.7.71	82,339
7	172.16.11.64	172.16.11.64	76,398
8	172.16.2.60	172.16.2.60	74,409
9	172.16.11.79	172.16.11.79	72,081
10	172.16.22.55	172.16.22.55	69,716
11	172.16.0.64	172.16.0.64	64,114
12	172.16.192.100	172.16.192.100	62,109
13	172.16.7.67	172.16.7.67	59,767
14	172.16.12.52	172.16.12.52	55,798
15	172.16.22.59	172.16.22.59	53,805
16	172.16.7.62	172.16.7.62	51,756
17	172.16.17.53	172.16.17.53	47,723
18	172.16.11.63	172.16.11.63	44,321
19	172.16.0.51	172.16.0.51	41,123
20	172.16.22.61	172.16.22.61	41,079

Ilustración 3. Fuente: Departamento de Sistemas - Universidad Técnica de Babahoyo

Amenazas

Se examinaron las amenazas detectadas en la red, incluyendo la presencia de malware, botnets e intrusiones. Estos resultados proporcionan información crítica sobre los riesgos a los que podría estar expuesta la red, permitiendo una evaluación más profunda de las implicaciones de seguridad.



Botnet Detected

#	Botnet Name	Counts
1	LaplasClipper.Botnet	117
2	SystemBC.Botnet	75
3	Mirai.Botnet	51
4	Andromeda.Botnet	8
5	Loki.Botnet	1
6	Mozi.Botnet	1

Botnet Victims

#	Victim Name (or IP)	Counts
1	172.16.198.111	117
2	172.16.14.57	4
3	41.40.78.177	3
4	41.34.162.234	3
5	197.41.222.178	2
6	156.200.214.117	2
7	71.166.44.14	2
8	159.89.115.98	2
9	159.89.203.160	2
10	143.110.250.126	2
11	170.64.144.204	2
12	172.16.14.59	2

Ilustración 4. Fuente: Departamento de Sistemas - Universidad Técnica de Babahoyo

Entrevista con el departamento de Sistemas

Durante la entrevista realizada con representantes del departamento de sistemas de la universidad, se obtuvo información valiosa que complementa los resultados del análisis de tráfico.

En cuanto a la estructura de la red, se utiliza una configuración de red en malla. Esta red maneja diversos sistemas, entre los que destaca el Sistema Académico Integrado y las aulas virtuales. Estos sistemas albergan información crítica, como calificaciones, asistencias, sílabos y matrículas, fundamentales para el funcionamiento institucional.

En términos de seguridad, se implementa un Next Generation Firewall Fortinet y un sistema de detección de intrusiones. Se prioriza la apertura de protocolos necesarios y el bloqueo de los demás, lo que resulta en políticas de seguridad más claras y controladas. Antes de la implementación de seguridad, en el pasado ocurrieron incidentes de seguridad informática, como *defacement*, *ransomware* y ataques de denegación de servicio.

Las principales amenazas cibernéticas se centran en el escaneo de puertos,

denegación de servicios y malware. Además, se considera la posibilidad de implementar medidas de seguridad en dispositivos BYOD en el futuro.

En cuanto a la identificación y mitigación de riesgos, se realiza un proceso autónomo, en el cual el sistema bloquea y alerta sobre riesgos identificados. Para mejorar la seguridad, se sugiere migrar a una versión 2.0 de sistemas y abordar el tema de BYOD con una mayor inversión en seguridad.

DISCUSIÓN DE RESULTADOS

Para la realización del análisis y evaluación de los riesgos de seguridad informática se deben seguir una serie de pasos.

Identificación de activos

En la Universidad Técnica de Babahoyo, se han identificado activos de información y recursos de red que desempeñan un rol crucial en las operaciones de la institución. Entre estos se incluyen servidores y bases de datos. Además, los datos sensibles almacenados, como información estudiantil y docente, son esenciales para el funcionamiento institucional.

Identificación de amenazas y vulnerabilidades

Las amenazas y vulnerabilidades identificadas incluyen una amplia gama de riesgos potenciales que podrían afectar la seguridad informática de la Universidad. Se destaca la presencia o exposición a malware sobre todo mediante el uso web de los usuarios, lo que puede comprometer la integridad y confidencialidad de los sistemas y datos. Además, la detección de botnets y la posibilidad de intrusiones indican la existencia de amenazas externas que podrían aprovecharse de vulnerabilidades en la red. Se observa también la posibilidad de acceso no autorizado a través de VPN y la detección de eventos de alta severidad.

Evaluación de riesgos

La evaluación de riesgos implica analizar tanto la probabilidad como el impacto en caso de que ocurra una amenaza. En el caso de las amenazas de malware, la probabilidad puede considerarse moderada debido a la alta actividad de tráfico, mientras que el impacto potencial es significativo en términos de pérdida de datos y funcionalidad. Los botnets también presentan una probabilidad moderada y un impacto potencial alto.

Priorización de riesgos

Basándose en la evaluación de riesgos, se priorizan las amenazas identificadas según su nivel de riesgo. Las amenazas de malware y botnets se consideran críticas debido a su potencial para afectar la confidencialidad, integridad y disponibilidad de datos y sistemas. Las amenazas de acceso no autorizado también son prioritarias, ya que podrían comprometer sistemas cruciales. Estas prioridades guiarán la asignación de recursos y la implementación de medidas de mitigación.

Identificación y evaluación de controles existentes

Se revisan los controles de seguridad existentes en la Universidad Técnica de Babahoyo, como firewalls, sistemas de detección de intrusos y políticas de acceso. Se valúa su eficacia en la mitigación de los riesgos identificados. Por ejemplo, a través de un incidente previo donde se experimentó una interrupción del sistema durante un examen utilizando la herramienta Kali Linux, se identificó una brecha en las políticas de seguridad interna. En este caso, la falta de políticas internas permitió que los estudiantes afectaran inadvertidamente la red interna, lo que resultó en una caída del sistema. Tras este incidente, se implementaron medidas y políticas internas más sólidas para prevenir futuros problemas y asegurar la continuidad de los servicios de manera segura.

Propuesta de medidas de mitigación

Se proponen medidas de mitigación específicas para abordar los riegos identificados. Estas medidas pueden incluir:

Mejora de políticas de seguridad: Se propone la revisión y actualización de las políticas de seguridad existentes para abordar las vulnerabilidades y amenazas identificada. Esto podría incluir la implementación de políticas más estrictas en cuanto al acceso y el uso de recursos de red, así como la definición de políticas de seguridad interna y externa para prevenir incidentes similares al mencionado.

Actualización de software: Se recomienda implementar un proceso regular de actualización de software para garantizar que las vulnerabilidades conocidas estén parchadas y que los sistemas estén protegidos contra amenazas comunes.

Educación en seguridad informática para los usuarios: Dado que la vulnerabilidad más grande en los sistemas y redes son los usuarios, se sugiere la implementación de programas de educación en seguridad informática para sensibilizar a los usuarios sobre las mejores prácticas de seguridad, la identificación de amenazas y el manejo adecuado de situaciones de riesgo.

Los resultados de este estudio encuentran coherencia con las nociones fundamentales del marco conceptual de seguridad informática. Por ejemplo, en el análisis del consumo de ancho de banda y patrones de aplicaciones, se destaca la presencia de picos en la cantidad de sesiones en ciertos días. Este patrón podría indicar actividad anómala o intentos de ataque, lo cual es congruente con la idea de que las redes LAN enfrentan constantemente amenazas externas.

El análisis del uso web revela comportamientos de navegación de usuario que merecen atención en términos de seguridad. La identificación de usuarios con actividad inusualmente alta y el consumo de ancho de banda por categorías específica arroja luz sobre posibles riesgos. La categorización de sitios bloqueados, como publicidad o juegos, coincide con los riesgos comunes en la navegación web, lo que subraya la importancia de gestionar estos aspectos para proteger la red.

La evaluación de amenazas resulta esencial en la seguridad informática. Los hallazgos relacionados con la detección de botnets e intrusiones resaltan los riesgos a

los que la red de la universidad de medidas de mitigación más robustas. Estos resultados también ofrecen una base sólida para un análisis más profundo de los posibles impactos y consecuencias asociadas con estas amenazas.

Aunque los resultados validan muchas de las suposiciones del marco conceptual, es vital abordar las discrepancias y limitaciones. Por ejemplo, la identificación de usuarios más activos no debe considerarse automáticamente como riesgosa, ya que algunos usuarios pueden tener roles que requieren un mayor uso de recursos. Esto sugiere la necesidad de una evaluación más detallada y personalizada de los perfiles de riesgo.

La evaluación de riesgos a través del análisis de tráfico en las redes LAN ha brindado información crítica para fortalecer la seguridad informática. Los hallazgos resaltan la importancia de una vigilancia constante y la implementación de medidas proactivas para mitigar las amenazas identificadas. Basándonos en estos resultados, se recomienda desarrollar estrategias de seguridad específicas, como actualizaciones de software, políticas de acceso, capacitación de usuarios, para mejorar la resiliencia de la red.

CONCLUSIONES

En el proceso de análisis y evaluación de riesgos de seguridad informática en las redes de área local de la Universidad Técnica de Babahoyo, se han logrado identificar, evaluar y proponer medida de mitigación para abordar amenazas y vulnerabilidades potenciales. El presente estudio se ha enfocado en cumplir con los objetivos planteados, cuyo propósito era analizar y evaluar los riesgos presentes en la red, identificar posibles vulnerabilidades y proponer soluciones efectivas para fortalecer la seguridad informática en la institución.

El análisis del consumo de ancho de banda y patrones de aplicaciones en la red ha revelado aspectos fundamentales en relación con la seguridad. La detección de picos en la cantidad de sesiones en días específicos sugiere la posibilidad de actividad anómala o intentos de ataque. La identificación de usuarios con actividad inusualmente alta y el consumo de ancho de banda por categorías específicas también han proporcionado *insights* valiosos para abordar posibles riesgos.

La evaluación de amenazas ha permitido identificar posibles puntos vulnerables en la red. La presencia de botnets o la exposición a malware mediante el uso web destaca la necesidad de una protección más rigurosa contra estas amenazas, así como la importancia de mantener los sistemas actualizados para prevenir vulnerabilidades conocidas. Es crucial destacar la necesidad de contar con licencias adecuadas de antivirus y soluciones de seguridad, La falta de estas medidas de protección representa un riesgo significativo para la integridad y confidencialidad de los sistemas y datos de la universidad.

La revisión de controles de seguridad existentes en la Universidad, en particular el incidente previo donde se experimentó una interrupción del sistema durante una prueba utilizando Kali Linux, resalta la importancia de implementar políticas de seguridad sólidas tanto internas como externas. Esta experiencia ha demostrado la necesidad de considerar los riesgos internos y tomar medidas para prevenir futuras interrupciones.

En consecuencia, se han propuesto medidas de mitigación específicas para abordar los riesgos identificados. La mejora de políticas de seguridad, la actualización de software y la educación en seguridad informática para los usuarios son estrategias esenciales para fortalecer la seguridad de la red. Estas medidas, respaldadas por los hallazgos del análisis, tienen como objetivo mejorar la resiliencia de la red y prevenir futuras vulnerabilidades.

RECOMENDACIONES

Considerando la presencia de malware y botnets en la red, se sugiere implementar soluciones de seguridad robustas, incluyendo software antivirus y antimalware actualizados. Estas herramientas deben ser acompañadas de análisis y actualizaciones regulares para prevenir amenazas emergentes.

Para fortalecer la seguridad, es esencial mejorar las restricciones sobre el uso de redes en plataformas específicas y revisar las políticas de acceso y control de red, junto con medidas como la autenticación de dos factores. Esto garantiza un acceso más seguro a la información sensible y reduce los riesgos en plataformas potencialmente riesgosas.

Para abordar la vulnerabilidad de los usuarios se propone la implementación de programas de educación es seguridad informática. Estos programas deben enfocarse en las mejores prácticas de seguridad y la identificación de amenazas, adaptándose a las amenazas en constante evolución.

Para prevenir vulnerabilidades conocidas, se recomienda establecer un proceso de actualización de software regular y parches en todos los sistemas y aplicaciones de la red. Esto ayudará a mitigar riesgos asociados con vulnerabilidades obsoletas.

La implementación de políticas internas y externas sólidas es esencial. Basado en experiencias previas, se sugiere definir políticas de seguridad interna y externa para prevenir interrupciones y garantizar la continuidad de los servicios.

REFERENCIAS

Casetto, O. (2023, February 1). *Cybersecurity Threats: Everything you Need to Know*. Exabeam. https://www.exabeam.com/information-security/cyber-security-threat/

Cep, E. (2019). *Cuerpo Auxiliar. Junta de Comunidades de Castilla-La Mancha. Temario. Vol. III*. EDITORIAL CEP. https://books.google.com.ec/books?id=J2GRDwAAQBAJ

CEPAL. (2020, December 18). *Protección de los datos - Gestión de datos de investigación - Biblioguias at Biblioteca CEPAL, Naciones Unidas*. Biblioguias at Biblioteca CEPAL, Naciones Unidas.

Coppola, M. (2023, May 8). *Seguridad informática: qué es, tipos y características*. Blog de HubSpot. https://blog.hubspot.es/website/que-es-seguridad-informatica#:~:text=Descarga%20gratis%20aqu%C3%AD-,Qu%C3%A9%20es%20la%20seguridad%20inform%C3%A1tica,da%C3%B1o%20o%20acceso%20no%20autorizado.

Corao, F. P., & Vanegas, M. P. (2023). *Administración de servicios web. Anatomía del Internet*. Marcombo. https://books.google.com.ec/books?id=dtavEAAAQBAJ

Escudero, P. C., Domínguez, J. M. C., Cano, J. C. G., Venegas, D. G., & Blanco, J. M. (2022). *CFGB Operaciones auxiliares para la configuración y la explotación 2022*. Editorial Editex. https://books.google.com.ec/books?id=ESd1EAAAQBAJ

Grupo Atico34. (2023, May 16). *Confidencialidad, integridad y disponibilidad de los datos*. https://protecciondatos-lopd.com/empresas/confidencialidad-integridad-disponibilidad/#Que_es_la_disponibilidad

Hernandez, Y. (2022, April 18). *¿Qué es una amenaza en seguridad Informática y cómo prevenirla?* Dongee. https://www.dongee.com/tutoriales/que-es-una-amenaza-en-seguridad/

Hino, M. C., Przeybilovicz, E., & Coelho, T. R. (2019). Bring your own device (BYOD): entendendo uma nova prática no ambiente acadêmico. *Acta Scientiarum. Education*, *41*, 1–13. https://www.redalyc.org/articulo.oa?id=303360435038

Irwin, L. (2020, July 20). *Risk terminology: Understanding assets, threats and vulnerabilities*. Vigilant Software.

OnTek. (2019, August 29). *¿Qué es? | Tríada CID (Confidencialidad, Integridad y Disponibilidad)*.

Postigo Palacios, A. (2020). *Seguridad informática (Edición 2020)*. Ediciones Paraninfo, SA. https://books.google.es/books?id=UCjnDwAAQBAJ&lpg=PR5&ots=-H1VhqaPl6&dq=seguridad%20inform%C3%A1tica&lr&hl=es&pg=PR5#v=onepage&q=seguridad%20inform%C3%A1tica&f=false

Rausand, M., & Haugen, S. (2020). *Risk Assessment: Theory, Methods, and Applications*. Wiley. https://books.google.com.ec/books?id=4yrPDwAAQBAJ

Sangfor Technologies. (2022, September 7). *What is Network Traffic Analysis NTA? Definition, Explanation and Tools*. https://www.sangfor.com/blog/cybersecurity/what-is-network-traffic-analysis-definition-explanation-and-tools

SecurityScorecard. (2021, May 26). *How to Identify and Prepare for Network Security Threats and Vulnerabilities*.

ANEXOS

Anexo A: Entrevista a los Encargados del Departamento de Sistemas

A continuación, se presenta la transcripción completa de la entrevista realizada a dos encargados del departamento de sistemas:

¿Cuál es la estructura de la red de área local en la Universidad Técnica de Babahoyo?

La red de área local en la Universidad Técnica de Babahoyo está configurada en forma de red en malla.

¿Qué tipos de datos y sistemas se manejan en la red de área local? ¿Qué información se considera crítica o sensible para la universidad?

En la red de la universidad, manejamos datos relacionados con la gestión institucional, como calificaciones, asistencias, sílabos, matrículas, entre otros. También se gestionan aulas virtuales y sistemas secundarios, como bibliotecas virtuales, sistemas de incidencias y sistemas antiplagio.

La información que se considera crítica o sensible es principalmente la de las personas que integran la universidad. Esta información está protegida por leyes.

¿Cuáles son las medidas de seguridad informática actualmente implementadas en la red de área local? ¿Existen políticas de seguridad establecidas?

Implementamos un Next Generation Firewall Fortinet, que incluye políticas de seguridad para el tráfico entrante y saliente. También configuramos un IDS/IPS para bloquear amenazas de intrusos utilizando la base de datos del firewall.

¿Cuáles son las políticas más utilizadas?

Priorizamos abrir y bloquear protocolos específicos en función de nuestros servicios. Las políticas más comunes son de permitir y bloquear.

¿Han ocurrido incidentes de seguridad informática en la red en el pasado? ¿Cuáles han sido los principales desafíos y amenazas enfrentadas?

Antes de implementar el equipo de seguridad, experimentamos *defacement* en nuestra página web, *ransomware*, virus dañinos y ataques de denegación de servicio. También hemos enfrentado amenazas de escaneo de puertos y malware.

Además, debido a la ausencia de políticas de seguridad interna, durante una prueba, los estudiantes de sistemas realizaron un ataque de denegación de servicio con la herramienta Kali Linux y el sistema se cayó.

¿Se realiza un análisis de tráfico en la red actualmente? ¿Qué herramientas o métodos se utilizan para realizar este análisis?

Sí, el firewall Fortinet realiza análisis de tráfico y genera reportes semanales.

¿Qué tipo de comportamientos anómalos o patrones de tráfico podrían indicar posibles riesgos de seguridad en la red?

Debido a que la red es grande analizamos el tráfico usando el motor de análisis del firewall Fortinet para identificar vulnerabilidades y amenazas. El propio equipo busca comportamientos inusuales que puedan indicar posibles riesgos. El proceso detección y mitigación de riesgos es autónomo.

¿Cuáles son las principales amenazas cibernéticas o riesgos de seguridad que se consideran relevantes para la red de área local de la universidad?

Una de las principales amenazas que siempre hemos tenido es el escaneo de puertos desde el exterior, así como la denegación de servicios y los malware y virus porque en la universidad no contamos con licencias de antivirus y malware en todas las máquinas lo que puede ser una vulnerabilidad, pero se mitiga con el firewall.

¿Existen dispositivos BYOD (Bring Your Own Device) conectados a la red? ¿Cómo se gestionan estos dispositivos en términos de seguridad?

Aunque sería muy beneficioso implementar este tipo de seguridad a la red de la universidad, de momento no existe. Tener este tipo de seguridad requeriría de mayor inversión

¿Cómo se mantienen actualizados en cuanto a las últimas tendencias y amenazas en seguridad informática?

Para estar actualizados siempre es importante conocer qué máquinas o equipos están a la vanguardia en lo que respecta a la seguridad informática. El equipo que adquirimos es uno de los más eficientes en seguridad informática y actualizan constantemente su base de datos en cuanto a los riesgos emergentes. Investigamos constantemente qué equipos están más actualizados de forma que podamos adquirir los mejores y así estar más seguros.

¿Qué recomendaciones o propuestas tienen para mejorar la seguridad informática en la red de área local?

Es recomendable que nuestros sistemas se actualicen a la versión 2.0 debido a los riesgos emergentes y cambios en la programación. Además, estamos planeando dotar a toda la universidad de acceso a internet para evitar que los estudiantes conecten routers no autorizados a la red LAN, lo que puede crear vulnerabilidades.

Anexo B: Informe del Análisis de Tráfico de Red

Consumo de ancho de banda y aplicaciones

Top 20 Users by Bandwidth

#	User (or IP)	Source IP	Bytes	Sent	Received
1	172.16.2.49	172.16.2.49	948.28 GB		
2	172.16.7.51	172.16.7.51	93.83 GB		
3	172.16.13.51	172.16.13.51	76.61 GB		
4	172.16.11.64	172.16.11.64	64.28 GB		
5	172.16.2.60	172.16.2.60	43.56 GB		
6	172.16.17.53	172.16.17.53	42.20 GB		
7	172.16.2.55	172.16.2.55	37.84 GB		
8	172.16.22.55	172.16.22.55	37.67 GB		
9	172.16.12.52	172.16.12.52	33.48 GB		
10	172.16.2.20	172.16.2.20	30.29 GB		
11	172.16.192.100	172.16.192.100	29.96 GB		
12	172.16.22.54	172.16.22.54	29.87 GB		
13	172.16.22.61	172.16.22.61	29.77 GB		
14	172.16.22.56	172.16.22.56	28.99 GB		
15	172.16.7.71	172.16.7.71	27.48 GB		
16	172.16.0.213	172.16.0.213	27.16 GB		
17	172.16.11.84	172.16.11.84	26.56 GB		
18	172.16.17.52	172.16.17.52	24.89 GB		
19	172.16.48.116	172.16.48.116	22.22 GB		
20	172.16.11.52	172.16.11.52	22.04 GB		

Ilustración 5. Fuente: Universidad Técnica de Babahoyo - DTSI

Top 20 Usuarios por Ancho de Banda

Esta información es esencial para identificar posibles comportamientos anómalos que podrían indicar actividades no autorizadas o amenazas de seguridad. Puede ayudar a detectar posibles brechas en la seguridad y a tomar medidas preventivas para mitigar riesgos y salvaguardar la integridad de la red.

Uso web

Reporte semanal UTB

Top 20 Most Blocked Users

#	User (or IP)	Hostname	Requests
1	172.16.22.61	172.16.22.61	353,706
2	172.16.20.53	172.16.20.53	142,035
3	172.16.201.120	172.16.201.120	136,439
4	172.16.22.65	172.16.22.65	92,803
5	172.16.198.100	172.16.198.100	87,428
6	172.16.22.63	172.16.22.63	71,809
7	172.16.200.10	172.16.200.10	44,083
8	172.16.7.67	172.16.7.67	40,352
9	172.16.193.113	172.16.193.113	40,091
10	172.16.197.201	172.16.197.201	38,122
11	172.16.201.14	172.16.201.14	24,322
12	172.16.12.52	172.16.12.52	24,031
13	172.16.11.63	172.16.11.63	23,686
14	172.16.200.181	172.16.200.181	23,170
15	172.16.194.76	172.16.194.76	23,102
16	172.16.196.89	172.16.196.89	22,067
17	172.16.196.161	172.16.196.161	19,941
18	172.16.200.175	172.16.200.175	18,259
19	172.16.11.78	172.16.11.78	17,539
20	172.16.197.28	172.16.197.28	16,421

Ilustración 6. Fuente: Universidad Técnica de Babahoyo - DTSI

Top 20 Usuarios Más Bloqueados

Identificar a los usuarios más bloqueados puede ayudar a detectar posibles intentos de acceder a sitios web maliciosos, contenido no permitido u otras actividades que representen un riesgo para la seguridad de la red. Analizar esta información es fundamental para mantener un entorno de red seguro y garantizar que los usuarios cumplan con las políticas establecidas.

Top 20 Most Blocked Categories

#	Category	Requests
1	Advertising	2,620,174
2	Games	301,208
3	Proxy Avoidance	91,466
4	Potentially Unwanted Program	87,383
5	Internet Radio and TV	23,205
6	Malicious Websites	19,793
7	Dating	14,921
8	Travel	3,427
9	Pornography	3,212
10	Other Adult Materials	2,733
11	Gambling	2,162
12	Phishing	1,100
13	Illegal or Unethical	1,076
14	Brokerage and Trading	919
15	Web Chat	272
16	Lingerie and Swimsuit	224
17	Personal Vehicles	159
18	Plagiarism	116
19	Advocacy Organizations	89
20	Alternative Beliefs	56

Ilustración 7. Fuente: Universidad Técnica de Babahoyo - DTSI

Top 20 Categorías Más Bloqueadas

Estas categorías representan los tipos de contenido o actividades que han sido restringidos o bloqueados por razones de seguridad. Identificar las categorías más bloqueadas puede ayudar a comprender qué tipos de contenido representan mayores riesgos para la red y qué medidas de seguridad deben reforzarse.

Amenazas

Intrusions Detected

#	Attack Name	Severity	CVE-ID	Counts
1	MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution	Crítico	CVE-2017-0144	270
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Crítico	CVE-2019-9082,CVE-2018-20062	85
3	udp_flood	Crítico		55
4	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Crítico	CVE-2017-9841	37
5	Zyxel.zhttpd.Webserver.Command.Injection	Crítico		17
6	Dasan.GPON.Remote.Code.Execution	Crítico	CVE-2018-10561,CVE-2018-10562	10
7	Andromeda.Botnet	Crítico		8
8	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	Crítico	CVE-2015-2051,CVE-2019-10891	7
9	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Crítico		7
10	WordPress.HTTP.Path.Traversal	Crítico	CVE-2019-9618,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	3

Ilustración 8. Fuente: Universidad Técnica de Babahoyo - DTSI

Detecciones de Intrusiones

Las intrusiones detectadas pueden incluir intentos de acceso no autorizado, escaneo de puertos, tráfico malicioso y otros comportamientos sospechosos que podrían representar amenazas para la seguridad de la red. El monitoreo y análisis de las detecciones de intrusiones son esenciales para identificar posibles ataques en tiempo real y tomar medidas para mitigarlos. Esta información contribuye significativamente a mantener la integridad y seguridad de la red.

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

Babahoyo, 17 de agosto del 2023
D-FAFI-UTB-00552-2023

Ingeniero.
Marcos Oviedo Rodríguez, Ph.D.
RECTOR DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO
En su despacho. -

Agradeceré proceder con el trámite que corresponde
Ing. Marcos Oviedo Ph. D.
RECTOR UTB
22/08/2023

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 **ANGIE SCARLETTE CASTRO ROMAN** con cédula de identidad No. **1207881283** estudiante de la Carrera de Ingeniería en Sistemas de Información. matriculada en el proceso de titulación en el periodo junio – octubre 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional universitario de tercer nivel como Ingeniera en Sistemas de Información, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su proyecto. en el departamento de sistemas de la Universidad Técnica de Babahoyo, el cual titula: **"ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA A TRAVES DEL ANÁLISIS DE TRÁFICO EN REDES DE ÁREA LOCAL DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO
c.c: Archivo

UNIVERSIDAD TÉCNICA DE BABAHOYO
DECANATO

UNIVERSIDAD TÉCNICA DE BABAHOYO
DIRECCIÓN DE TECNOLOGÍAS
22 AGO 2023
HORA
RECIBIDO

UNIVERSIDAD TÉCNICA DE BABAHOYO
RECTORADO
FECHA 22/08/2023 HORA 9:56
SECRETARIA