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

PROCESO DE TITULACIÓN DICIEMBRE 2022 – ABRIL 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:

"ESTUDIO COMPARATIVO DE LAS INFRAESTRUCTURAS DE LAS TI Y HERRAMIENTAS INFORMATICAS PARA MITIGAR ATAQUES DISTRIBUIDOS DE DENEGACION DE SERVICIO"

ESTUDIANTE:

SANCHEZ CONTRERAS JOEL ANDRES

TUTOR:

HARRY ADOLFO SALTOS VITERI

AÑO 2023

Contenido

Resumen

El estudio comparativo analiza diferentes infraestructuras de TI y herramientas de software utilizadas para combatir los ataques DDoS. El propósito es evaluar las fortalezas y debilidades de cada solución disponible y proporcionar información útil para elegir la mejor opción para proteger su red contra ataques DDoS. El estudio también tuvo como objetivo comprender los principales tipos de ataques DDoS y los métodos utilizados para prevenir y mitigar estos ataques.

El tema principal es la importancia de la seguridad informática en las empresas. Estos ataques pueden ser catastróficos para una organización, por lo que una evaluación exhaustiva de la infraestructura de TI y el hardware utilizado es esencial para identificar posibles vulnerabilidades y áreas que necesitan mejorar. Además, es importante implementar medidas y soluciones de seguridad que puedan prevenir o mitigar los ataques DDoS y crear un plan de respuesta DDoS sólido. La razón de esto es la importancia particular de la seguridad de TI en el mundo actual, especialmente con el número creciente de ataques DDoS y la necesidad de proteger los sitios web de las empresas para evitar pérdidas financieras y daños a la reputación.

Palabras claves: ataques DDoS, seguridad informática, infraestructuras de TI, herramientas informáticas, prevención de ataques, mitigación de ataques, plan de respuesta a incidentes, evaluación exhaustiva, vulnerabilidades, medidas de seguridad.

Planteamiento del problema

Hoy en día los ataques más comunes y lo que los hackers utilizan para impedir el funcionamiento de un sitio web es el ataque de denegación de servicios o también conocido en sus siglas como DDoS, De tal manea hay que reconocer cuando se está siendo víctima de dicho ataque, de esta manera podemos saber qué hacer y que tecnología aplicar para no sufrir dicho ataque informático, existen las herramientas y (TI) o llamadas tecnologías de la información, mediante las indicaciones correctas podemos tomar muchas medidas de prevención, en este caso de estudio vamos a realizar una comparación entre las infraestructuras TI y tecnologías informáticas.

La problemática en este caso es el aumento de los ataques de denegación de servicio distribuidos (DDoS) que afectan a las infraestructuras de TI de las empresas. Los ataques DDoS se han vuelto cada vez más comunes en los últimos años y pueden tener graves consecuencias para las empresas, como la pérdida de ingresos, la disminución de la productividad y la pérdida de la confianza del cliente.

En este contexto, las empresas necesitan implementar soluciones efectivas para mitigar los ataques DDoS y proteger sus infraestructuras de TI. Esto implica la adopción de herramientas y tecnologías que les permitan detectar y bloquear los ataques DDoS en tiempo real.

Sin embargo, hay una gran variedad de herramientas y soluciones disponibles en el mercado, y cada una tiene sus propias ventajas y desventajas. Además, el costo de estas soluciones puede ser alto, por lo que las empresas deben evaluar cuidadosamente sus opciones antes de tomar una decisión de inversión.

A medida que las páginas web se expanden, también lo hace la incertidumbre dentro de ellas, por lo que la palabra seguridad se ha convertido en una prioridad para

proteger la información que se muestra en las páginas web, y también es una forma en que las empresas se anuncian a los usuarios. En seguridad informática, el ataque es una forma de socar el arduo trabajo de los informáticos y de las grandes y medianas empresas al impedir que defiendan la integridad de la información y el no repudio en la transmisión con base en las matemáticas discretas y la teoría de la información; y su propósito es proteger la información almacenada y la información transmitida a través de Internet.

Otro aspecto que se puede ver afectada es la gestión de la información es muy importante en las empresas u organizaciones actuales porque es pública y se encuentra en una página web el contenido de la información o archivos por lo consiguiente se puede manipular y mostrar a conveniencia. Todos los tipos de páginas web pasan por diferentes etapas ya sean de mejora o modificar algún punto importante o agregar algo nuevo y se debe tener cuidado en cada etapa de modificación, ya que puede verse comprometida en cualquier momento.

Justificación

La justificación de este tema es la importancia crítica de la seguridad informática en la actualidad, especialmente en el contexto del creciente número de ataques DDoS. Se realizará este caso de estudio debido a que los ataques DDoS son una amenaza constante para las organizaciones que dependen de los servicios web, y pueden causar interrupciones costosas en los servicios y dañar la reputación de la organización o empresas.

Con este caso de estudio se comprenderá como mitigar los problemas causados por ataques DDoS para las grandes, medianas y pequeñas empresas, por lo tanto, se sugiere una solución que incluya realizar capacitaciones a los miembros de las empresas sobre la infraestructura o las herramientas informáticas utilizadas para limitar esta libertad que tienen los atacantes y tener una idea clara de lo que se debe hacer antes de convertirse en víctima de un ataque. Actualmente, es necesario mantener y conocer las soluciones informáticas y establecer ciertas reglas de seguridad para no ser víctima de ataques, pues esto es muy importante porque protegemos y evitamos ataques a su sitio web o servidor por parte de intrusos informáticos.

El estudio comparativo de la infraestructura de TI y las herramientas informáticas para combatir los ataques distribuidos de denegación de servicio es un tema importante y relevante, dado el creciente número de ciberataques en los últimos años. Los ataques de denegación de servicio (DDoS) son uno de los métodos más comunes utilizados por los ciberdelincuentes para comprometer los sistemas informáticos de una organización. Por ejemplo, los ataques DDoS pueden tener graves consecuencias para las empresas. Tales como interrupciones del servicio, pérdida de datos y rendimiento reducido. Por lo tanto, existe la necesidad de una infraestructura de TI y herramientas efectivas para mitigar el impacto de estos ataques.

Objetivos

Objetivo general

- Determinar por medio de una comparación cual infraestructura o herramienta es la adecuada para atenuar la solución de la problemática, la cual es disminuir los ataques distribuidos de denegación de servicios.

Objetivos específicos

- Investigar los diferentes tipos de ataques distribuidos de denegación de servicio (DDoS) y promover su impacto en las empresas y organizaciones.
- Identificar y comparar las diferentes infraestructuras de las TI y herramientas informáticas utilizadas para mitigar los ataques DDoS, evaluando su eficacia y eficiencia.
- Realizar un análisis de coste-beneficio de las diferentes soluciones de infraestructura y herramientas informáticas para mitigar los ataques DDoS, con el fin de determinar la mejor opción para empresas y organizaciones de diferentes tamaños y presupuestos.

Línea de investigación

Esta investigación o estudio de caso está enfocado en la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, sostenida por la sublínea usada que es, investigación de redes y tecnologías inteligentes de software y hardware que permita aplicar lo que es la investigación cualitativa ya que estudia todas las cualidades del ataque distribuido, por lo tanto se consiguió utilizar de la misma manera el método investigativo deductivo, mismo que permitió la obtención de una información actualizada y de esta manera llegar a los dilemas que afectan a las páginas web o servidores web que hoy en día son víctimas de los atacantes, una de las técnicas que se uso fue las entrevistas para así recopilar información valiosa para la solución de este estudio de caso.

Marco conceptual

Infraestructura de TI

La infraestructura de TI es la colección de hardware, software, redes y servicios que mantienen una organización en funcionamiento. En el contexto de la ciberseguridad, la infraestructura de TI juega un papel importante en la protección de los sistemas y datos de una organización de los ataques distribuidos de denegación de servicio. (Schreider, 2018).

Según (al C. , 2018), La infraestructura de TI es una colección de tecnologías, servicios y recursos necesarios para respaldar los procesos de una organización. Según Gartner, una de las empresas líderes en investigación de TI, la infraestructura de TI se puede dividir en dos categorías: infraestructura básica e infraestructura avanzada. La infraestructura central incluye los recursos necesarios para operar y mantener el entorno de TI de una organización, como servidores, redes, sistemas de almacenamiento y software central. La infraestructura avanzada, por otro lado, se refiere a tecnologías más avanzadas que permiten a las organizaciones aumentar la productividad, la seguridad y la innovación. Estas tecnologías pueden incluir inteligencia artificial, análisis de datos avanzados, automatización de procesos y soluciones IoT.

Seguridad de la infraestructura de TI

Se inicializa en la protección de la infraestructura de TI contra amenazas internas y externas. Según (Mattord, 2016), La seguridad de su infraestructura de TI es esencial para garantizar la seguridad, la integridad y la disponibilidad de los sistemas y datos críticos de su organización, y para cumplir con las leyes y regulaciones de seguridad y protección de datos.

Virtualización de servidores

Se enfoca en el uso de la tecnología de virtualización para optimizar la gestión de servidores en una organización. Según (Seetharaman, 2017), la virtualización de servidores permite un mejor uso de los recursos de hardware, una gestión de servidores más flexible y una implementación más eficiente de nuevas aplicaciones y servicios.

Gestión de redes y comunicaciones

Se centra en la gestión y configuración de redes y comunicaciones en la organización. Según (Ross, 2005), la gestión de la red y la comunicación es esencial para el éxito de la empresa, ya que mejora la comunicación y la colaboración entre los grupos de trabajo, así como mejorar la eficiencia de las tareas y proyectos.

¿Qué es la infraestructura de TI ?

Según (Iranmanesh, 2019), la infraestructura de tecnología de la información (TI) se define como "un conjunto de recursos que incluyen hardware, software, redes y servicios, que proporcionan soporte para la creación, almacenamiento, procesamiento y entrega de datos y aplicaciones en una organización". Un modelo de soporte de decisiones para la selección de infraestructura de computación en la nube.

Instalaciones en las infraestructuras TI

"La instalación de infraestructura de TI es un proceso crítico que requiere planificación detallada, gestión de proyectos y coordinación cuidadosa entre equipos de TI y otros grupos de la organización. Una instalación bien planificada puede garantizar que la infraestructura de TI esté disponible, segura y capaz de cumplir con los objetivos de la organización". (Musthaler, 2017)

Enlaces y telecomunicaciones en las TI

Los enlaces de telecomunicaciones son la columna vertebral de la infraestructura de TI, ya que permiten la conexión de dispositivos y redes distribuidas geográficamente. Una gestión adecuada de los enlaces de telecomunicaciones es esencial para garantizar una conexión confiable y segura entre las diferentes partes de la organización. (Horwitz, 2017)

Almacenamiento

"Según (Crump, 2017), el almacenamiento es una de las áreas críticas de la infraestructura de TI, ya que permite la conservación, protección y acceso a los datos de la organización. Las soluciones de almacenamiento deben ser escalables, seguras y rentables para satisfacer las necesidades cambiantes de la organización en términos de capacidad, velocidad y rendimiento".

Uso de Máquinas Virtuales en las TI

Las máquinas virtuales son una tecnología clave para la gestión de la infraestructura de TI, ya que permiten la consolidación de servidores físicos, la creación de entornos aislados y la implementación rápida de aplicaciones. Las soluciones de virtualización deben ser escalables, seguras y de fácil administración para maximizar los beneficios de la tecnología". (Posey, 2017)

Sistemas Operativos

"Los sistemas operativos son la base de la infraestructura de TI, ya que cuentan con el entorno necesario para ejecutar aplicaciones y servicios. Los sistemas operativos deben ser seleccionados cuidadosamente para satisfacer las necesidades de la

organización en términos de seguridad, compatibilidad, escalabilidad y facilidad de administración".(Michael, 2018)

Run time

"Run time es el período durante el cual un programa de software se ejecuta en una computadora. El run time puede ser crítico en aplicaciones en tiempo real y en aplicaciones de alta disponibilidad, donde es importante minimizar el tiempo de inactividad y maximizar el rendimiento. La solución de run time deben ser escalables, seguras y de fácil administración para garantizar un funcionamiento óptimo de la aplicación" Los run times deben ser seleccionados cuidadosamente para satisfacer las necesidades de la aplicación en términos de compatibilidad, rendimiento y seguridad". (Rouse, 2018)

Datos

Según (Sahasrabuddhe, 2017), los datos son el corazón de la transformación digital y la toma de decisiones basada en datos se ha convertido en una necesidad para las organizaciones. La gestión de datos incluye la recopilación, almacenamiento, procesamiento, análisis y presentación de datos para obtener información valiosa y mejorar la eficiencia y eficacia de los procesos de negocio".

Firewalls

"Un firewall es un dispositivo de seguridad de red que supervisa y controla el tráfico de red entrante y saliente en función de las políticas de seguridad definidas. Su objetivo principal es proteger la red de amenazas externas e internas, restringiendo el acceso no autorizado a recursos de red y datos confidenciales". (Juyal, 2017)

Las formas de protección de la red

La protección de red es un conjunto de técnicas y medidas diseñadas para garantizar la seguridad y privacidad de una red de computadora, protegiéndola de amenazas externas e internas. Según (Adnane, 2020), Proteger la red es crucial para cualquier empresa, ya que los ataques cibernéticos se vuelven más sofisticados y peligrosos. Se utilizan varias herramientas y tecnologías para una protección eficaz, por ejemplo: Cortafuegos, Sistema de detección y prevención de intrusiones (IDS/IPS), Sistema de prevención de pérdida de datos (DLP), Control de acceso y autenticación, Cifrado de datos y VPN, etc. Estas herramientas ayudan a detectar y detener a los intrusos, el malware y otras amenazas, y mantienen la privacidad y la seguridad de los datos mientras viajan por la red.

La ciberseguridad se refiere a la implementación de medidas de seguridad para proteger los sistemas y datos de una organización de los ataques distribuidos de denegación de servicio. Esto puede incluir la implementación de firewalls, filtros de paquetes y otras medidas de seguridad.(Muniz, 2017).

Protección de la red contra ataques DDoS:

(Osterman, 2018), Describir la creciente importancia de la protección contra los ataques DDoS en un mundo cada vez más conectado. Osterman explica cómo los ataques DDoS pueden afectar la disponibilidad de la red y los servicios en línea, y describe varias soluciones de protección DDoS como: B. Soluciones y servicios de seguridad basados en la nube del proveedor de servicios de seguridad administrados (MSSP).

Protección de la red contra amenazas de malware:

(Shackleford, 2017)**,** Describe cómo puede usar técnicas de ciencia de datos para detectar y proteger su red contra malware. Shackleford explica cómo usar las técnicas de análisis de datos para detectar patrones de tráfico sospechosos, detectar comportamientos inusuales de los usuarios y monitorear la actividad de la red en busca de signos de infección de malware dañino.

Mitigación de ataques DDoS

La prevención de ataques DDoS se refiere a tomar medidas para mitigar el impacto de los ataques de denegación de servicio distribuidos. Estas medidas pueden incluir la creación de redes redundantes, la implementación de técnicas de equilibrio de carga y la implementación de herramientas de mitigación de DDoS. (Lu, 2018).

La mitigación de ataques DDoS (Distributed Denial of Service) es un conjunto de técnicas y medidas utilizadas para proteger una red de computadoras de ataques que buscan saturarla con un tráfico anormalmente elevado, impidiendo que los usuarios legítimos puedan acceder a los recursos de la red. Según (al N. , 2021), Los ataques DDoS se están convirtiendo en una amenaza cada vez más común y pueden tener graves consecuencias, por ejemplo, para las empresas afectadas. b Lucro cesante, pérdida de reputación e interrupciones del servicio. Se utilizan varios métodos para prevenir ataques DDoS, como: B. Detección temprana, segmentación de red, regulación, filtrado de paquetes, redirección de tráfico y colaboración con un proveedor de servicios de seguridad administrados (MSSP). Estos métodos permiten detectar y bloquear el tráfico malicioso, protegiendo así la red y asegurando el acceso a los recursos por parte de los usuarios autorizados.

Mitigación de ataques DDoS mediante la implementación de políticas de seguridad:

Las políticas de seguridad pueden ser utilizadas para reducir el impacto de los ataques DDoS en una red. (Almeshekah, 2018), explica cómo se pueden usar las políticas de seguridad para restringir el tráfico entrante, configurar umbrales de tráfico y restringir el acceso a recursos de red críticos.

Mitigación de ataques DDoS mediante el uso de soluciones de protección:

(Radware, 2019), Describe cómo utilizar las soluciones de protección DDoS para mitigar el impacto de los ataques DDoS en la red. Radware explica cómo las soluciones de protección DDoS pueden proporcionar protección en tiempo real contra ataques, ayudar a identificar y bloquear el tráfico malicioso y proporcionar información sobre el tráfico de la red para un análisis más detallado.

Mitigación de ataques DDoS mediante el uso de blockchain

Según (X. Xu, 2017), Blockchain DDoS Protection es una nueva técnica que utiliza la tecnología blockchain para proteger los servicios en línea de los ataques DDoS. En este enfoque, se utiliza una red blockchain distribuida para almacenar las identidades de los clientes y los recursos de la red, lo que proporciona autenticación y verificación seguras. Además, se utiliza un algoritmo de consenso distribuido para coordinar y sincronizar la protección contra ataques DDoS. Los resultados muestran que este método puede prevenir con éxito los ataques DDoS y garantizar una protección eficaz de los servicios de Internet.

Sistema de detección de intrusiones (IDS)

Los sistemas de detección de intrusos son herramientas de seguridad que monitorean sistemas y redes en busca de actividad sospechosa. Estos sistemas son útiles para detectar y mitigar ataques distribuidos de denegación de servicio. (Bejtlich, 2017).

Análisis de tráfico en IDS

El análisis de tráfico es el estudio y seguimiento del tráfico de la red para detectar posibles ataques o comportamientos inusuales. En el contexto de los sistemas de detección de intrusos, el análisis de tráfico se utiliza para identificar patrones de tráfico maliciosos o inusuales que podrían indicar un ataque. Uno de los métodos utilizados en el análisis de movimiento es la detección de anomalías, que busca patrones de movimiento inusuales en comparación con la captura de movimiento normal. Otro método es el reconocimiento de patrones, que busca patrones de tráfico conocidos que podrían indicar un ataque.(Mell, 2016)**.**

IDS basado en firmas

El IDS basado en firmas es un tipo de IDS que busca patrones específicos, llamados firmas, para detectar posibles ataques. Estas firmas son patrones de tráfico específicos que coinciden con los patrones de tráfico generados por un ataque conocido. Los sistemas IDS basados en firmas utilizan bases de datos de firmas para comparar el tráfico de red entrante con firmas conocidas para identificar posibles ataques. (Bejtlich R. , 2018)

Detección de Intrusiones Basada en Comportamiento

Según (Shenglong Chen, 2017), La detección de intrusiones basada en el comportamiento es una técnica que utiliza algoritmos de aprendizaje automático para

analizar el comportamiento de los usuarios y los sistemas en una red. Este enfoque se centra en la detección de comportamientos inusuales que pueden indicar una amenaza potencial. Estos sistemas pueden adaptarse a nuevas amenazas, haciéndolos más efectivos que los sistemas basados en firmas. Sin embargo, también pueden producir falsos positivos si no se configuran correctamente.

Sistemas de Detección de Intrusiones Basados en Red (NIDS)

Los sistemas de detección de intrusos en la red (NIDS) son herramientas implementadas en puntos específicos de una red para monitorear el tráfico y detectar amenazas potenciales. Estos sistemas analizan el tráfico de red en busca de comportamientos inusuales y pueden detectar ataques que afectan a múltiples sistemas. NIDS puede detectar amenazas en toda la red, pero es posible que no detecte ataques dirigidos a sistemas individuales. (Sathya, 2018)

Protección de infraestructura critica

La Protección de Infraestructura Crítica (CIP) es un enfoque integral diseñado para prevenir, detectar y responder a las amenazas a los activos y sistemas críticos que son fundamentales para la vida de nuestros clientes, la seguridad nacional y la prosperidad. La protección de la infraestructura crítica se está volviendo cada vez más importante en todo el mundo a medida que las infraestructuras críticas, como las redes de energía, los sistemas financieros, las redes de transporte y los sistemas de atención médica, se vuelven cada vez más importantes, se vuelven interdependientes y vulnerables a una variedad de amenazas, incluidos los desastres naturales, los accidentes, el error humano, y ciberataques. (L.S. Di Pietro, 2017).

Según (L.S. Di Pietro, 2017) PIC implica identificar y evaluar riesgos, implementar medidas de seguridad y monitorear y responder en caso de una crisis. Esto incluye el uso de tecnologías avanzadas como sensores de vigilancia, sistemas de seguridad física, sistemas de control de acceso, software de análisis de datos, sistemas de detección de intrusos y sistemas de seguridad de red. También incluye la colaboración entre agencias gubernamentales, empresas y organizaciones de la sociedad civil para garantizar la protección integral de la infraestructura crítica.

Seguridad en la Nube para Infraestructuras Críticas

La seguridad en la nube para la infraestructura crítica es un enfoque para proteger los sistemas críticos y a los datos almacenados en la nube. Las soluciones de seguridad en la nube pueden incluir cifrado de datos, autenticación de usuarios, control de acceso y monitoreo continuo. Estas soluciones pueden ayudar a reducir el riesgo de ataques cibernéticos y garantizar la disponibilidad e integridad de los sistemas en la nube de misión crítica..(Xhafa, 2019).

Análisis de Vulnerabilidades en Infraestructuras Críticas

Según (Irfan, 2017), El escaneo de vulnerabilidades de infraestructura crítica es el proceso de identificar y evaluar vulnerabilidades potenciales en sistemas y redes críticas. Estas vulnerabilidades pueden incluir puertos abiertos, contraseñas débiles o software obsoleto. El análisis de vulnerabilidades es una parte importante de la seguridad de la infraestructura crítica, ya que le permite identificar vulnerabilidades y repararlas antes de que los atacantes las exploten.

Sistemas de Protección de Infraestructuras Críticas Basados en la Telemetría

Los sistemas de protección de infraestructura crítica basados en telemetría son aquellos que utilizan sensores y equipos de monitoreo para recopilar datos de sistemas y redes de misión crítica. (E. Aravantinou, 2018) Estos sistemas pueden analizar estos datos en tiempo real para detectar amenazas potenciales y tomar medidas para proteger los sistemas críticos. La telemetría puede incluir información sobre el uso del ancho de banda, el tráfico de la red y el consumo de energía.

La infraestructura de TI se refiere a la estructura del hardware, el software y los recursos necesarios para mantener y administrar el entorno tecnológico. Esto incluye servidores, almacenamiento, redes, bases de datos, sistemas operativos y software de aplicación. La seguridad de la infraestructura de TI se refiere a las medidas tomadas para proteger la infraestructura de TI de amenazas como ataques de piratas informáticos, malware y robo de datos. Esto incluye medidas como firewalls, software de seguridad, autenticación de usuarios, encriptación de datos y monitoreo de actividades sospechosas.

La virtualización de servidores es una tecnología que le permite ejecutar múltiples servidores virtuales en un solo servidor físico. Esto permite una mejor utilización de los recursos, más flexibilidad y menores costos. La instalación de infraestructura de TI implica configurar físicamente los componentes de hardware y los entornos que los contienen, como centros de datos, salas de servidores y armarios de cables.

Un firewall es un dispositivo que protege una red informática del acceso no autorizado, malware y otros tipos de ataques. Hay diferentes tipos de cortafuegos, como cortafuegos de red, cortafuegos de aplicaciones y cortafuegos de hardware. Hay diferentes formas de proteger su red de ataques DDoS, que son ataques en los que se utilizan varios dispositivos para inundar un sitio web o una red con tráfico.

Marco metodológico

La técnica o método investigativo que se usó en este caso de estudio para persuadir o recopilar información es de tipo descriptivo ya que por medio de una entrevista a personas profesionales en servicio activo se logró recopilar una serie de información y de la misma manera generar respuestas a las preguntas de parte de los entrevistados, las personas entrevistadas narraron sus experiencias las cuales han adquirido con forme laboran en su ámbito de trabajo.

La metodología descriptiva suele utilizarse en investigaciones sociales y de mercado para recopilar información detallada sobre un fenómeno o situación en particular.

Se estaría realizando entrevistas a varias personas que se especialicen en la seguridad o que sean ingenieros en sistemas con experiencia en seguridad informática, para recopilar información detallada sobre que o cual herramienta o infraestructura TI, es esencial para mitigar ataques de denegación de servicios.

Existen varias herramientas e infraestructuras TI, para prevenir un ataque DDoS. Luego de la recopilación de la información hacemos una comparación entre las respuestas de cada pregunta para por medio de eso determinar cuál es más favorable y así asimilar que el estudio comparativo se esté realizando adecuadamente.

Se logró de la misma manera aplicar el uso de tablas comparativas para determinar que herramienta o infraestructura es la adecuada para prevenir o mitigar un ataque DDoS.

Resultados

Una vez que se haya realizado la entrevista a las personas profesionales en el ámbito laboral de tecnologías informáticas e infraestructuras TI, se obtuvieron los siguientes resultados.

En base a la interrogante:

a. **¿Cuáles son las herramientas más efectivas para mitigar los ataques de denegación de servicio?**

El ingeniero Jorge Benítez Administrador de Red en la empresa Paris net, indica la siguiente respuesta: La herramienta más efectiva para la mitigación de los ataques DDoS es la buena configuración del Firewall de nuestro RouterBoard ya que de esta forma podemos monitorear el trafico entrante y así podemos decidir que entra y que no a la red.

En base a la respuesta el firewall es la primera línea de defensa contra los ataques de red y puede ayudar a bloquear el tráfico malicioso antes de que llegue a la red.

La interrogante:

b. **¿Cuáles son las diferencias principales entre las soluciones de seguridad de red y las soluciones de seguridad de aplicación para prevenir los ataques de denegación de servicio?**

La respuesta del ingeniero Jorge Benítez Administrador de Red en la empresa Paris net es: Toma el nombre de firewall perimetral, se puede decir que una de sus principales diferencias es el nivel en el que operan.

En base al marco conceptual se concluye que el firewall perimetral opera en un nivel diferente en comparación con otros tipos de firewalls

La interrogante:

c. **¿Qué factores deberían tenerse en cuenta al seleccionar una solución de seguridad de denegación de servicio para una organización?**

El ingeniero Jorge Benítez Administrador de Red en la empresa Paris net, dice: Es muy importante tener un ancho de banda suficiente para cuando hagan inundación de tráfico no afecte de manera crítica.

Como enfoque principal, es importante implementar múltiples capas de defensa para proteger la red contra las amenazas actuales y emergentes.

d. **¿Cuáles son los requisitos de hardware y software para implementar soluciones de seguridad de denegación de servicio?**

El ingeniero Jorge Benítez Administrador de Red en la empresa Paris net, presenta la siguiente respuesta: Cisco ASA, Fortinet, Palo Alto. También el firewall perimetral que se coloca en la entrada de una red para proteger las amenazas externas.

En resumen, el ingeniero jorge Benitez enfoca que los requisitos son fortinet, Cisco, y palo alto. Contrastando con la teoría del marco conceptual, concuerdo con él, ya que su aplicación es de suma importancia en las empresas para preservar la integridad.

La siguiente persona con conocimientos en seguridad informática y redes nos da las siguientes respuestas a las mismas interrogantes:

La interrogante:

a. **¿Cuáles son las herramientas más efectivas para mitigar los ataques de denegación de servicio?**

La primera respuesta por el ingeniero Jahir Navarro asistente de sistemas en el GAD Municipal, a la interrogante **a** es: Algunas de las herramientas más efectivas para mitigar los ataques de denegación de servicio son: Filtros de tráfico, Firewalls, Sistemas de detección y prevención de intrusiones (IDS/IPS), Servicios de mitigación de ataques de denegación de servicio (DDoS).

Es importante recordar que ninguna solución es perfecta y que los ataques DDoS están en constante evolución.

La interrogante:

b. ¿Cuáles son las diferencias principales entre las soluciones de seguridad de red y las soluciones de seguridad de aplicación para prevenir los ataques de denegación de servicio?

La segunda respuesta por el ingeniero Jahir Navarro asistente de sistemas en el GAD Municipal, a la interrogante **b** es: Las soluciones de ciberseguridad se centran en proteger la red y el tráfico entrante, mientras que las soluciones de seguridad de aplicaciones se centran en proteger las aplicaciones y los servicios web. La solución de seguridad de red incluye un firewall, IDS/IPS y filtro de tráfico, mientras que la solución de seguridad de aplicaciones incluye un sistema de protección de aplicaciones web, un servicio de protección DDoS y un servicio de protección API.

Cada una de estas herramientas tiene su propio propósito y es importante considerarlas en conjunto para crear una estrategia de seguridad completa.

La interrogante:

c. ¿Qué factores deberían tenerse en cuenta al seleccionar una solución de seguridad de denegación de servicio para una organización?

La tercera respuesta por el ingeniero Jahir Navarro asistente de sistemas en el GAD Municipal, a la interrogante **c** es: Los factores que deben tenerse en cuenta incluyen: Escalabilidad, Flexibilidad, Facilidad de implementación, Costo.

Según lo investigado los factores mencionados son realmente importantes a considerar al momento de seleccionar una solución de seguridad para una infraestructura de TI.

La interrogante:

d. ¿Cuáles son los requisitos de hardware y software para implementar soluciones de seguridad de denegación de servicio?

La tercera respuesta por el ingeniero Jahir Navarro asistente de sistemas en el GAD Municipal, a la interrogante **d** es: Los requisitos de hardware y software para implementar soluciones de denegación de servicio dependen de la solución específica que esté utilizando. Sin embargo, algunas soluciones pueden requerir hardware especializado, como equipo anti-DDoS, mientras que otras pueden implementarse como software en un servidor existente.

Es importante considerar las necesidades específicas de la organización antes de seleccionar una solución

En base a la investigación se logró desarrollar estas tablas comparativas costo-beneficios la cual muestra cuales son las mejores opciones para mitigar ataques DDoS, por medio de estas tablas desarrolladas nos podemos dar cuenta que herramienta o componente de la infraestructura es mejor.

Estrategia 1

ESTRATEGIA 1					
Componente de la infraesti	Modelo o Marca	Características	Cantidad	Costo unitar	Costo total
Servidores	Dell PowerEdge R740	Cuenta con una arquitectura escalable	2	$10,000	$20,000
Almacenamiento	NetApp AFF A220	Capacidad de almacenamiento de 10TB	1	$30,000	$30,000
Red de datos	Cisco Catalyst 9300	Capacidad de conexión de hasta 48 puertos.	2	$5,000	$10,000
Seguridad de la red	Palo Alto Networks PA-3220	Capacidad de inspección de tráfico de hasta 20 Gbps.	1	$25,000	$25,000
Virtualización	VMware vSphere Standard	Capacidad de virtualización de hasta 64 CPUs y 512GB de F	1	$3,000	$3,000
Monitoreo y gestión de la r	SolarWinds Network Performance I	Monitoreo de redes y aplicaciones, alertas en tiempo real	1	$8,000	$8,000
Licencias de software	Microsoft Windows Server Standar	Sistema operativo para servidores con capacidades de virtu	4	$1,000	$4,000
Total	-	-	-	-	$100,000

Esta tabla destaca por incluir un componente de seguridad de red de alta gama, el Palo Alto Networks PA-3220, lo que indica que se ha considerado la seguridad como una prioridad en la infraestructura de TI. Además, incluye marcas conocidas y bien establecidas como Dell, NetApp, Cisco y VMware, lo que sugiere una inversión en equipos de alta calidad y rendimiento. En resumen, la elección de componentes confiables y de alta calidad, incluido un componente de seguridad de red de alta gama, indica una infraestructura de TI sólida y confiable y menos costosa que otras.

La infraestructura más adecuada para protegerse contra los ataques DDoS depende de los requisitos específicos de seguridad de su red y de los recursos disponibles. Debe

usar una combinación de herramientas y tecnologías para brindar una protección integral contra los ataques DDoS.

Estrategia 2

ESTRATEGIA 2					
Componente de la infraestructura	**Modelo o Marca**	**Caracteristica**	**C**	**Costo unitario**	**Costo total**
Servidores	HPE ProLiant DL360 Gen10	Procesador Intel Xeon 6242R, 32 GB de memoria RAM	2	$11,000	$22,000
Almacenamiento	Dell EMC Unity 300	Capacidad de almacenamiento de 20 TB, compatibilidad con RAID	1	$35,000	$35,000
Red de datos	Juniper Networks EX2300-C	Puertos de cobre y fibra óptica, capacidad de apilamiento virtual	2	$2,500	$5,000
Seguridad de la red	Fortinet FortiGate 100E	Firewall de última generación, protección contra amenazas avanza	1	$15,000	$15,000
Virtualización	VMware vSphere Essentials Plus	Licencia para 3 hosts, capacidades de alta disponibilidad	1	$5,500	$5,500
Monitoreo y gestión de la red	PRTG Network Monitor	Monitoreo en tiempo real, alertas personalizables	1	$2,500	$2,500
Licencias de software	Microsoft Windows Server Datacenter	Licencias para 4 servidores, incluye virtualización	4	$6,000	$24,000
Ingeniero en seguridad			1	$2,000	$2,000
Microtik Routerboard	RB1100AHx4	Cuatro núcleos de CPU, 1 GB de memoria RAM	1	$500	$500
Total	-				$111.500

La tabla muestra una lista de componentes de infraestructura, con la cantidad, el costo unitario y el costo total. La lista incluye dos servidores HPE ProLiant DL360 Gen10, un almacenamiento Dell EMC 300, una red de datos Juniper Networks EX2300-C, un firewall Fortinet FortiGate 100E, virtualización VMware vSphere Essentials Plus, supervisión de red de PRTG, licencias de software del centro de datos del servidor de Microsoft Windows y una placa de enrutador Microtik RB1100AHx4. El costo total de la infraestructura es de $109,500, lo que la hace más costosa que la tabla anterior.

La tabla es más costosa porque utiliza componentes de infraestructura más avanzados y potentes que la tabla anterior, como los servidores HPE ProLiant DL360 Gen10 con procesadores Intel Xeon 6242R y 32 GB de memoria RAM, el almacenamiento Dell EMC 300 con capacidad de almacenamiento de 20 TB y compatibilidad con RAID, y el firewall Fortinet FortiGate 100E con protección contra

amenazas avanzadas. Estos componentes son más costosos, sin embargo, ofrecen un mejor rendimiento y seguridad. Además, la lista incluye una placa de enrutador adicional, lo que también contribuye al costo total.

Discusión de resultados

Con base en la discusión de los resultados, la respuesta a la primera pregunta de los resultados, que fue respondida por el ingeniero Jorge Benítez, es una solución viable y efectiva para reducir los ataques de Denegación de Servicio (DDoS). La configuración adecuada del firewall del enrutador permite a los administradores de red monitorear el tráfico entrante y bloquear el tráfico malicioso o no deseado. Además, una buena configuración de firewall puede ayudar a prevenir futuros ataques al implementar políticas de seguridad sólidas.

Sin embargo, vale la pena señalar que existen otras herramientas y estrategias que se pueden utilizar para mitigar el impacto de los ataques DDoS, como: Sistemas de prevención y detección de intrusos (IDS/IPS), sistemas de protección DDoS basados en la nube y servicios de red de entrega de contenido (CDN).

Según las respuestas de Jorge Benítez son correctas en el sentido de que una de las diferencias claves entre una solución de seguridad de red y una solución de seguridad de aplicaciones es la medida en que operan.

Las soluciones de ciberseguridad como el firewall perimetral se enfocan en proteger toda la red al monitorear y controlar el tráfico que ingresa y sale de la red. Estas soluciones están diseñadas para detectar y bloquear ataques DDoS antes de que lleguen a un servidor o aplicación.

La sustentabilidad hecha por el ingeniero Jorge Benítez respecto a la importancia del ancho de banda suficiente como un factor a tener en cuenta al tener una solución anti-DDoS es precisa. Estas soluciones pueden consumir una gran cantidad de recursos para prevenir ataques.

En cuanto a los requisitos de hardware y software para implementar una solución anti-DDoS, el ingeniero enumeró varias empresas de seguridad de redes como Cisco ASA, Fortinet y Palo Alto, que son bien conocidas por sus soluciones de seguridad. Es importante investigar y evaluar diferentes proveedores y soluciones para determinar qué proveedor y solución se adapta mejor a las necesidades de su negocio. Además, se debe considerar la escalabilidad y flexibilidad de la solución para que pueda adaptarse a las necesidades comerciales cambiantes.

El ingeniero también mencionó el firewall periférico, que es una herramienta que protege la red contra amenazas externas. Sin embargo, debe tenerse en cuenta que un solo firewall puede no ser suficiente para proteger contra ataques DDoS y es posible que se requieran soluciones de seguridad DDoS adicionales para brindar una protección integral contra estos ataques.

La respuesta del ingeniero Jahir Navarro es correcta debido a que los factores a tener en cuenta al elegir una solución de protección contra denegación de servicio incluyen escalabilidad para satisfacer las necesidades de una organización en crecimiento, flexibilidad para adaptarse a requisitos específicos, facilidad de uso y facilidad de uso. junto con el presupuesto de la organización. Los requisitos de hardware y software pueden variar según la solución que esté utilizando, pero es importante que su hardware y software sean compatibles y cumplan con los requisitos mínimos del sistema para un rendimiento óptimo.

La respuesta del ingeniero Jahir Navarro proporcionó una descripción general de las herramientas y soluciones necesarias para protegerse contra los ataques de denegación de servicio. Al elegir una solución empresarial de denegación de servicio, tenga en cuenta la escalabilidad, la flexibilidad, la facilidad de implementación y el costo. Además, los requisitos de hardware y software varían según la solución que esté utilizando.

Conclusiones

La investigación de los diferentes tipos de ataques distribuidos de denegación de servicio (DDoS) ha demostrado que estos pueden tener un impacto significativo en la disponibilidad y el rendimiento de los sistemas y servicios de una empresa u organización. Es importante que las empresas estén conscientes de los distintos tipos de ataques DDoS y sus posibles consecuencias para que puedan tomar medidas adecuadas para prevenirlos y minimizar su impacto.

La identificación y comparación de las diferentes infraestructuras de TI y herramientas informáticas para mitigar los ataques DDoS muestra que existe una variedad de soluciones disponibles en el mercado. Estas soluciones varían en términos de su eficacia, eficiencia, facilidad de uso y costo. Por lo tanto, es importante que las empresas evalúen cuidadosamente sus necesidades y presupuesto para seleccionar la solución que mejor se adapte a sus necesidades.

El análisis de coste-beneficio de las diferentes soluciones de infraestructura y herramientas informáticas para mitigar los ataques DDoS es esencial para ayudar a las empresas y organizaciones a determinar la mejor opción para sus necesidades y presupuesto. Es importante considerar no solo el costo inicial de la solución, sino también los costos en curso, como los costos de mantenimiento y los costos operativos. La selección de la solución correcta puede ayudar a las empresas a minimizar el impacto de los ataques DDoS y proteger su reputación y su negocio.

Recomendaciones

Dadas estas recomendaciones las empresas deberían considerar la contratación de especialistas en seguridad informática para llevar a cabo una evaluación de riesgos y vulnerabilidades, con el fin de identificar posibles puntos débiles en su infraestructura de TI que puedan ser explotados por los ataques DDoS. Además, las empresas deberían llevar a cabo entrenamientos de concienciación de seguridad para todo su personal, de manera que estén preparados para reconocer y reportar cualquier actividad sospechosa que pueda indicar un posible ataque DDoS. Es importante que las empresas tomen medidas preventivas proactivas para reducir el riesgo de ataques DDoS y minimizar su impacto, en lugar de simplemente reaccionar a ellos después de que ocurran.

Es importante que las empresas consideren soluciones de seguridad que sean efectivas y eficientes, y que se adapten a sus necesidades específicas y presupuesto. Además, las empresas deberían considerar soluciones de seguridad basadas en la nube, que pueden proporcionar una protección más efectiva y escalable contra los ataques DDoS. Asimismo, las empresas se aseguren de contar con personal capacitado y recursos adecuados para administrar y mantener las soluciones de seguridad, para garantizar una protección óptima contra los ataques DDoS.

Las empresas deberían llevar a cabo un análisis detallado de coste-beneficio de las diferentes soluciones de infraestructura y herramientas informáticas para mitigar los ataques DDoS antes de tomar una decisión de compra.

También deben evaluar los costos potenciales asociados con la interrupción del negocio y la pérdida de ingresos en caso de un ataque DDoS exitoso. Por último, es importante que no comprometan la calidad de la solución de seguridad con el precio, ya que elegir una solución de seguridad inadecuada puede resultar en mayores costos a largo plazo.

Referencias

Adnane, M. B. (2020). Proteccion de red. *Una encuesta sobre las amenazas a la seguridad de la red, las soluciones y las futuras direcciones de investigación. .*

al, N. (2021). *Una revisión sistemática de la literatura sobre ataques distribuidos de denegación de servicio (DDoS) y técnicas de mitigación.*

Almeshekah, M. (2018). *"Mitigating Distributed Denial of Service Attacks: A Review of Defenses and Challenges".*

Beaver, K. (2018). *Beaver, K. (2018). Hacking for Dummies. John Wiley & Sons.*

Bejtlich, R. (2018). *: "The Practice of Network Security Monitoring: Understanding Incident Detection and Response" de Richard Bejtlich, publicado por No Starch Press.*

Bhuvaneswari, J. &. (2017). *A Study on Network Monitoring Tools Using Open Source Technologies. International Journal of Applied Engineering Research.*

Chuvakin, A. (2017). *Análisis de tráfico de red: ¿un componente imprescindible de la seguridad? Gartner.*

E. Aravantinou, M. M. (2018). *"Telemetry-based Critical Infrastructures Protection: A Comprehensive Review",.*

Irfan, d. D. (2017). *"Analysis of Vulnerabilities in Critical Infrastructure: A Comprehensive Review",.*

L.S. Di Pietro, A. O. (2017). *"Critical Infrastructure Protection: Requirements and Challenges".*

Lu, J. W. (2018). *"DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance".*

Mell, K. S. (2016). *"Guide to Intrusion Detection and Prevention Systems (IDPS)" (Special Publication 800-94), del National Institute of Standards and Technology (NIST).*

Muniz, J. (2017). *Security Operations Center: Building, Operating, and Maintaining Your SOC.*

Osterman, M. (2018). *La creciente importancia de la protección DDoS. Investigación de Ostermann.*

P. Sarigiannidis, I. G. (2018). *"DDoS attack mitigation using neural networks"*.

Radware. (2019). *Global Application & Network Security Report. Radware.*

Rao, H. R. (2018). *Network Monitoring Based on Flow Analysis: A Review. International Journal of Engineering & Technology*.

Sanders, C. (2018). *Applied Network Security Monitoring. Syngress.*

Sathya, S. S. (2018). *Survey of Network Intrusion Detection System.*

Shackleford, D. (2017). *Network Security Through Data Analysis. O'Reilly Media.*

Shenglong Chen, Z. W. (2017). *A Deep Learning Approach for Intrusion Detection System"*.

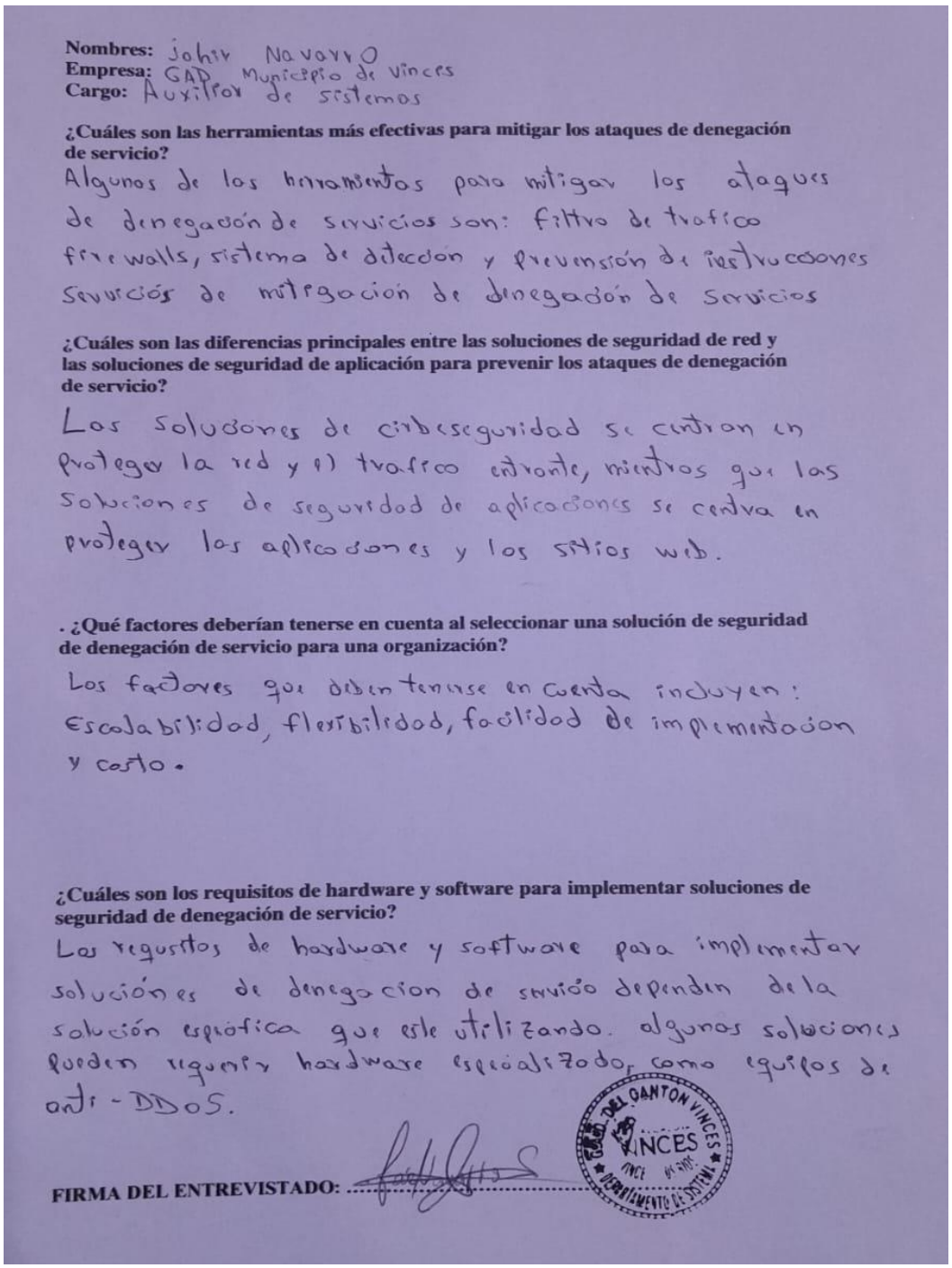
Srinivasan, R. y. (2018). *Network traffic analysis using wireshark. In 2018 International Conference on Computational Intelligence and Computing Research.*

X. Xu, Z. W. (2017). *"A Blockchain-based Approach to Enhancing DDoS Attack Mitigation"*.

Xhafa, A. A. (2019). *"Cloud Security for Critical Infrastructures: Survey and Future Directions"*.

Anexos

Entrevista sobre cuatro interrogantes a dos personas profesionales que se encuentran en el ámbito laboral, y tienen conocimiento sobre los ataques de denegación de servicios distribuidos.



Nombres: Johir Navarro
Empresa: GAD Municipio de Vinces
Cargo: Auxiliar de sistemas

¿Cuáles son las herramientas más efectivas para mitigar los ataques de denegación de servicio?

Algunos de las herramientas para mitigar los ataques de denegación de servicios son: filtro de trafico firewalls, sistema de diteccion y prevension de instrucciones Servicios de mitigacion de denegación de servicios

¿Cuáles son las diferencias principales entre las soluciones de seguridad de red y las soluciones de seguridad de aplicación para prevenir los ataques de denegación de servicio?

Las soluciones de ciberseguridad se centran en proteger la red y el trafico entrante, mientras que las soluciones de seguridad de aplicaciones se centra en proteger las aplicaciones y los sitios web.

. ¿Qué factores deberían tenerse en cuenta al seleccionar una solución de seguridad de denegación de servicio para una organización?

Los factores que deben tenerse en cuenta incluyen: Escalabilidad, flexibilidad, facilidad de implementacion y costo.

¿Cuáles son los requisitos de hardware y software para implementar soluciones de seguridad de denegación de servicio?

Los requisitos de hardware y software para implementar soluciones de denegacion de servicio dependen de la solución especifica que este utilizando. algunas soluciones pueden requerir hardware especializado, como equipos de anti-DDoS.

FIRMA DEL ENTREVISTADO: .....

GAD DEL CANTON VINCES
VINCES
DESARROLLO DE SISTEMAS

Nombres: Jorge Luis Benitez Hidalgo
Empresa: Atomic Net
Cargo: Administrador de Red

¿Cuáles son las herramientas más efectivas para mitigar los ataques de denegación de servicio?

La herramienta más efectiva para la mitigación de los ataques DDOS es la buena configuración del Firewall de nuestro router board ya que de esta forma podemos monitorear el trafico entrante y así podemos decidir que entra y que no a la red.

¿Cuáles son las diferencias principales entre las soluciones de seguridad de red y las soluciones de seguridad de aplicación para prevenir los ataques de denegación de servicio?

Toma el nombre de Firewall perimetral, se puede decir que una de sus principales diferencias es el nivel que operan.

. ¿Qué factores deberían tenerse en cuenta al seleccionar una solución de seguridad de denegación de servicio para una organización?

Es muy importante tener un ancho de banda suficiente para cuando hagan inundación de trafico no afecte de manera exetica

¿Cuáles son los requisitos de hardware y software para implementar soluciones de seguridad de denegación de servicio?

Cisco ASA, Fortinet, Paloalto, también el Firewall Perimetral que se coloca en la entrada de una red para proteger las amenazas externas

FIRMA DEL ENTREVISTADO: Jorge Benites


RIS.NET


RIS.NET

CERTIFICADO DE ANÁLISIS

magister

Trabajo final

2%

6% Texto entre comillas
< 1% similitudes entre comillas

2% Idioma no reconocido

Nombre del documento: TRABAJO FINAL.docx
ID del documento: f8c5c3bfae36b10349fbcb9e6daeb8b23da272fe
Tamaño del documento original: 1,16 Mo
Autor: Joel Sanchez Contreras

Depositante: Joel Sanchez Contreras
Fecha de depósito: 31/3/2023
Tipo de carga: url_submission
fecha de fin de análisis: 31/3/2023

Número de palabras: 6947
Número de caracteres: 45.969

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.utb.edu.ec | Análisis de vulnerabilidades en la red del isp: "cafanet" parroqu... 4 fuentes similares	< 1%		Palabras idénticas : < 1% (50 palabras)
2	Basurto-Trabajo Final caso de estudio.docx | Basurto-Trabajo Final caso de ... #867bf3 2 fuentes similares	< 1%		Palabras idénticas : < 1% (32 palabras)
3	hdl.handle.net | Contribuciones para la Detección de Ataques Distribuidos de Deneg...	< 1%		Palabras idénticas : < 1% (34 palabras)
4	dspace.utb.edu.ec | Analisís de factibilidad de un IDS (sistema de detección de intru...	< 1%		Palabras idénticas : < 1% (29 palabras)
5	www.infosegur.net | Que es un ataque de denegación de servicio distribuido (DDoS)... 8 fuentes similares	< 1%		Palabras idénticas : < 1% (22 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	hdl.handle.net | Metodología de implementación del estándar PCI-DSS en el diseño ...	< 1%		Palabras idénticas : < 1% (20 palabras)
2	www.redalyc.org | Técnicas de aprendizaje automático para la detección de intruso...	< 1%		Palabras idénticas : < 1% (11 palabras)
3	dspace.utb.edu.ec http://dspace.utb.edu.ec/bitstream/handle/49000/12662/E-UTB-FAFI-SIST.INF-000062.pdf?sequence=1	< 1%		Palabras idénticas : < 1% (10 palabras)
4	pcweb.info | Sistema de detección de intrusos, IDS, Intrusion detection system, qué es	< 1%		Palabras idénticas : < 1% (10 palabras)

Fuentes ignoradas

Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	MI CASO DE ESTUDIO JOEL SANCHEZ.docx | MI CASO DE ESTUDIO JOEL SAN... #2d2dc8	60%		Palabras idénticas : 60% (4204 palabras)
2	MI CASO DE ESTUDIO JOEL SANCHEZ.docx | MI CASO DE ESTUDIO JOEL SAN... #2de529	60%		Palabras idénticas : 60% (4189 palabras)