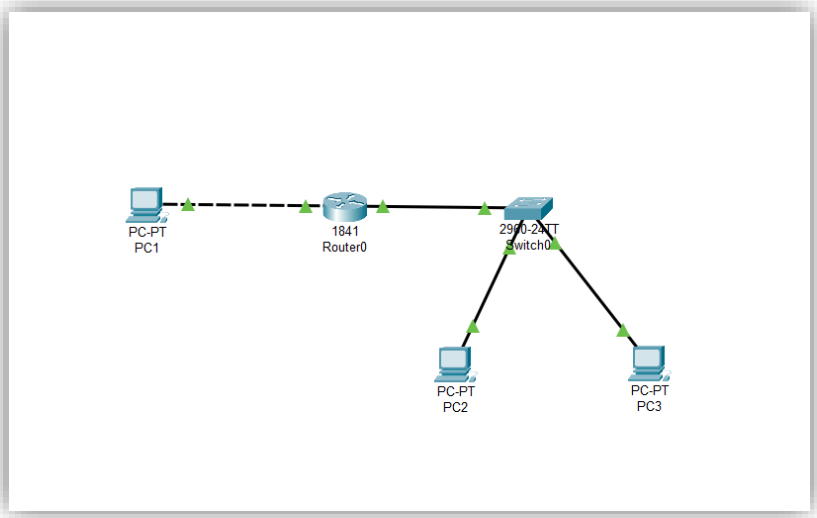
Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Laboratorio de Redes de Computadoras

3.2 Vulnerabilidades de seguridad en las redes



Alumno: Jesús Armando Espino Rodríguez
Matricula: 1844607

Profesora: Jorge Hernández Báez
Grupo: 032
Horario: 08:00 am a 9:00 am

Introducción:

En la actualidad a menudo se hace referencia a lo que se llama vulnerabilidades de seguridad en las redes de computadoras, esto es debido al auge de las redes mundiales, las operaciones, trámites, procesos, comunicaciones, etc., con ello, facilitan de mayor manera y ahorran tiempo y costos, pero de tal forma, existen riesgos en los cuales un usuario puede caer al no contar con una seguridad en las redes, pueden truncar sus actividades en la red, lo cual puede recaer en una acción perjudicial para él, por tal motivo es importante hacer una cultura de seguridad en las TIC´s.

- Investigar las problemáticas de seguridad que existen en las redes y qué tipo de implicaciones pueden tener si no se está preparado para ello, siendo así, las debilidades tecnológicas, de configuración o de políticas de seguridad.

Desafíos de Seguridad en Redes Informáticas: Preparación ante un Mundo Cibernético Amenazante

En la era digital actual, las redes informáticas se han convertido en el eje central de numerosas operaciones, trámites, procesos y comunicaciones a nivel mundial. Este fenómeno ha brindado innumerables beneficios, como una mayor eficiencia y ahorro de tiempo y costos. Sin embargo, junto con estos avances, también han surgido desafíos considerables en términos de seguridad cibernética.

Uno de los problemas más prominentes que enfrentan las redes informáticas es la proliferación de vulnerabilidades de seguridad. Estas vulnerabilidades pueden manifestarse en diversas formas, desde ataques de malware hasta técnicas sofisticadas de ingeniería social. Los ataques de malware, como virus, gusanos y troyanos, representan una amenaza significativa al comprometer la integridad de los sistemas y la confidencialidad de los datos. Por otro lado, los ataques de phishing, que implican el engaño de usuarios para obtener información confidencial, pueden resultar en robos de identidad y fraudes financieros devastadores.

Además de los ataques dirigidos específicamente, las redes informáticas también enfrentan desafíos derivados de debilidades tecnológicas, configuraciones inadecuadas y políticas de seguridad deficientes. Las vulnerabilidades en el software y hardware utilizados en una red pueden ser explotadas por atacantes para obtener acceso no autorizado, comprometiendo así la seguridad de toda la red. Asimismo, la falta de actualizaciones de seguridad y la configuración incorrecta de

dispositivos de red pueden dejar abiertas puertas traseras para los ciberdelincuentes, permitiéndoles eludir las medidas de seguridad y acceder a sistemas críticos.

Las implicaciones de no estar preparado para enfrentar estas amenazas son graves y pueden tener un impacto devastador en las organizaciones y los individuos. Desde la pérdida de datos confidenciales hasta la interrupción de servicios críticos, las consecuencias de un ataque cibernético exitoso pueden ser catastróficas. Además, los daños a la reputación de una empresa pueden ser difíciles de reparar y pueden llevar años reconstruir la confianza perdida de los clientes y socios comerciales.

Para mitigar estos riesgos y proteger la integridad de las redes informáticas, es fundamental adoptar una cultura de seguridad en las Tecnologías de la Información y Comunicación (TIC). Esto implica implementar medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones y cifrado de datos, así como mantener actualizados los sistemas y capacitar a los usuarios en prácticas seguras de seguridad informática. Además, es crucial establecer políticas de seguridad claras y promover una cultura organizacional que valore la seguridad cibernética como una prioridad estratégica.

- Analizar y explicar los métodos existentes que ofrecen la seguridad en las redes de computadoras

Métodos de Seguridad en Redes de Computadoras: Protegiendo los Cimientos de la Era Digital

En el contexto actual de interconexión global, donde las redes de computadoras desempeñan un papel fundamental en la conducción de operaciones comerciales, transacciones financieras y comunicaciones personales, la seguridad cibernética se ha convertido en una preocupación primordial. Para salvaguardar la integridad, confidencialidad y disponibilidad de los datos en estas redes, se han desarrollado y desplegado una variedad de métodos de seguridad. Estos métodos no solo protegen los activos digitales críticos, sino que también contribuyen a mantener la confianza y la estabilidad en el ciberespacio. En este ensayo, analizaremos y explicaremos algunos de los métodos más importantes que ofrecen seguridad en las redes de computadoras.

Uno de los métodos más básicos pero fundamentales para garantizar la seguridad en una red de computadoras es la autenticación de usuarios y dispositivos. La autenticación se refiere al proceso de verificar la identidad de un usuario o dispositivo antes de otorgar acceso a recursos de red. Esto se puede lograr mediante el uso de contraseñas, tokens de seguridad, biometría u otros mecanismos de autenticación multifactor. Al verificar la identidad de los usuarios y dispositivos, las organizaciones pueden controlar quién tiene acceso a la red y protegerla contra accesos no autorizados.

Otro método crucial para garantizar la seguridad en las redes de computadoras es el cifrado de datos. El cifrado implica convertir la información en un formato ilegible mediante el uso de algoritmos criptográficos. Solo aquellos que poseen la clave de cifrado adecuada pueden descifrar los datos y acceder a su contenido original. Esta técnica ayuda a proteger la confidencialidad de la información transmitida a través de la red, asegurando que solo los destinatarios autorizados puedan leerla.

Además de la autenticación y el cifrado, las redes de computadoras también se aseguran mediante el uso de firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS). Los firewalls actúan como barreras de seguridad entre una red interna y externa, controlando el tráfico entrante y saliente según reglas predefinidas. Por otro lado, los sistemas IDS/IPS monitorean activamente el tráfico de red en busca de actividades sospechosas o maliciosas y toman medidas para bloquear o mitigar las amenazas identificadas.

Además de estos métodos mencionados, también existen otras prácticas recomendadas para mejorar la seguridad en las redes de computadoras. Estas incluyen la segmentación de redes, el parcheo regular de sistemas y aplicaciones, la implementación de políticas de seguridad sólidas y la capacitación continua de los usuarios en prácticas seguras de seguridad informática.

- Desarrollar un cuadro sinóptico de los diferentes esquemas de seguridad en base a la encriptación y autenticación.

Esquemas de Seguridad

Encryptacion	*Autenticacion*
Encriptación simétrica: Este método utiliza una sola clave para cifrar y descifrar la información. Ambas partes deben compartir esta clave, lo que puede plantear desafíos en cuanto a la distribución segura de la clave. Ejemplos incluyen AES y DES	**Contraseñas:** Este método requiere que los usuarios ingresen una combinación de caracteres previamente establecida para verificar su identidad. Sin embargo, las contraseñas pueden ser vulnerables a ataques de fuerza bruta y phishing si no se gestionan de forma segura.
Encriptación asimétrica: También conocida como criptografía de clave pública, utiliza un par de claves, una pública y otra privada. La clave pública se comparte libremente, mientras que la clave privada se mantiene en secreto. Ejemplos incluyen RSA y ECC.	**Token de seguridad:** Estos dispositivos generan códigos aleatorios que se utilizan junto con las credenciales de usuario para autenticarse. Los tokens pueden ser físicos (dispositivos de hardware) o virtuales (aplicaciones móviles).
Hashing: Esta técnica convierte datos en una cadena de caracteres alfanuméricos de longitud fija. Es irreversible, lo que significa que no se puede obtener la información original a partir del hash. Se utiliza comúnmente para almacenar contraseñas de forma segura y para verificar la integridad de los datos. Ejemplos incluyen SHA-256 y MD5.	**Biometría:** Este método utiliza características únicas del individuo, como huellas dactilares, iris o rasgos faciales, para verificar su identidad. La biometría ofrece un alto nivel de seguridad, pero puede plantear preocupaciones sobre la privacidad y la precisión.
	Autenticación multifactor: Combina dos o más métodos de autenticación para verificar la identidad del usuario. Esto puede incluir una combinación de contraseñas, tokens de seguridad, biometría u otros factores. Proporciona una capa adicional de seguridad al requerir múltiples formas de verificación.

- Desarrollar un cuadro sinóptico de los diferentes esquemas de seguridad en base a la encriptación y autenticación.

La seguridad en redes es una preocupación crítica en la era digital actual. Adoptar un enfoque integral y proactivo hacia la seguridad cibernética es esencial para proteger los activos digitales y garantizar la confianza en el entorno de red. Al implementar medidas de prevención sólidas, capacitar a los usuarios y mantenerse al tanto de las últimas amenazas y vulnerabilidades, las organizaciones pueden mitigar los riesgos y fortalecer la seguridad de sus redes en el mundo cibernético de hoy en día.

Esta propuesta busca proporcionar un marco sólido para abordar los problemas de seguridad en las redes, pero es importante adaptarla a las necesidades y recursos específicos de cada organización.

Propuesta de Prevención de Problemas de Seguridad en Redes

- Realizar evaluaciones regulares de seguridad para identificar posibles vulnerabilidades en la red, los sistemas y las aplicaciones.
- Utilizar herramientas de escaneo de vulnerabilidades y realizar pruebas de penetración de manera periódica para identificar y remediar posibles puntos débiles.
- Desarrollar y aplicar políticas de seguridad claras y completas que aborden aspectos como el acceso de usuarios, la gestión de contraseñas, el cifrado de datos y la gestión de parches.
- Garantizar que todos los empleados y usuarios de la red estén capacitados en las políticas de seguridad y se adhieran a ellas en todo momento.
- Brindar capacitación regular a los empleados y usuarios sobre las mejores prácticas de seguridad informática, incluyendo la identificación de ataques de phishing, la creación de contraseñas seguras y la navegación segura por Internet.
- Fomentar una cultura de seguridad cibernética en toda la organización, donde la seguridad sea una responsabilidad compartida y todos estén alerta ante posibles amenazas.