
Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Redes y telecomunicaciones

Introducción

Hoy en día, los medios tecnológicos más utilizados son las redes y las telecomunicaciones, por ello son activos críticos y, por lo tanto, son blanco de atacantes para obtener y/o dañar información.

Estos elementos deben ofrecer en la información, disponibilidad, integridad y confidencialidad.

En este tema se dará a conocer cómo proteger las redes y las telecomunicaciones, como introducir los elementos básicos de una red y explicar los problemas de seguridad que rodean a las redes.

Explicación

Capas del modelo OSI

a. Capa de aplicación
Es el nivel último de la capa, el que aloja el programa de red que interactúa con el usuario.

b. Capa de presentación
Maneja los datos de la aplicación y los acomoda en un formato que pueda ser transmitido en una red.

c. Capa de sesión
Establece conexiones lógicas entre puntos de la red.

d. Capa de transporte
Maneja la entrega entre un punto y otro de la red de los mensajes de una sesión.

e. Capa de red
Maneja destinos, rutas, congestión en rutas, alternativas de enrutamiento, etcétera.

f. Capa de enlace de datos
Entrega los datos entre un nodo y otro en un enlace de red.

g. Capa de física
Define la conexión física de la red.

Explicación

Red de área local (**LAN**)

- Brindan conectividad de red para computadoras ubicadas en la misma área geográfica
- Un virus puede propagarse rápidamente a todos los sistemas.
- Los concentradores son simples dispositivos de red, que contienen varios enchufes.
- Los conmutadores son una alternativa mucho mejor que los concentradores, pueden realizar un filtrado inteligente.

Red de área amplia (**WAN**)

- Conectan sistemas en un área geográfica extensa.
- Es importante recordar que Internet es una red abierta.
- Un enrutador es un dispositivo que conecta dos o más redes e intercambia selectivamente paquetes de datos.

Explicación

Protocolo TCP/IP

El protocolo de control de transmisión (TCP)

- Permite a dos dispositivos de red establecer una conexión.
- Intercambia datos garantizando la entrega de datos en paquetes en el mismo orden en que fueron enviados.

El protocolo Internet (IP)

- Utiliza direcciones que son series de cuatro números llamados octetos.
- Con un formato de punto decimal por ejemplo: 255.5.164.58.

Explicación

Herramientas básicas de defensa de seguridad de red TCP / IP.

Firewall

Controla el flujo de tráfico de red.
Agrega un elemento de disuasión muy necesario.

VPN

Normalmente utiliza encriptación PPTP, SSL o IPSec

UTM

Filtro de URL.
Inspección de contenido.
Inspección de malware.

NAC

Software antivirus actualizado.
Host firewall.
Sistemas operativos compatibles.

Actividad

Investiga cuántas capas tiene el protocolo TCP/IP y qué capas de este protocolo equivalen a las capas del modelo OSI.

Realiza un esquema que permita relacionar las equivalencias entre ambos modelos.

Cierre

La importancia de conocer el modelo OSI y el protocolo TCP/IP son esenciales para lograr una interconexión de sistemas abiertos, así como para poder transmitir datos tanto en una red como en Internet.

Asimismo, conocer qué herramientas ofrecen seguridad en la red TCP/IP ayuda al administrador de seguridad de la información a tener el control del tráfico en la red.


Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Encriptación de la información

Introducción

La necesidad de proteger información digital como los datos que viajan en la red, discos duros, carpetas o incluso archivos, obliga a los estrategas de la seguridad de información a implementar técnicas de cifrado.

En este tema se abarcarán los conceptos de encriptación, así como las estrategias para transformar un mensaje legible en un formato que solo puedan leer los usuarios autorizados.

Explicación

Objetivos de seguridad usando criptografía

- Privacidad o confidencialidad
- Integridad
- Autenticación o identificación de la entidad
- Autenticación de mensajes
- Firma
- Control de acceso
- Certificación
- Sellado de tiempo
- Testimonio
- Propiedad
- Anonimato
- No repudio

Explicación

Tipos de cifrado

Cifrados de sustitución

- Reemplazan bits, letras o bloques de letras con diferentes bits, letras o bloques de letras.

  Estos son seleccionados cuidadosamente para resistir el criptoanálisis.

Cifrados de transposición

- En lugar de reemplazar el texto original, mueve los valores originales alrededor, los reacomoda para ocultar el texto original.

Explicación

Claves, espacio de claves y administración de claves

Claves criptográficas y espacio de claves
El conjunto de todas las claves posibles se conoce como espacio de claves, y cuanto mayor sea, más seguro será el algoritmo.

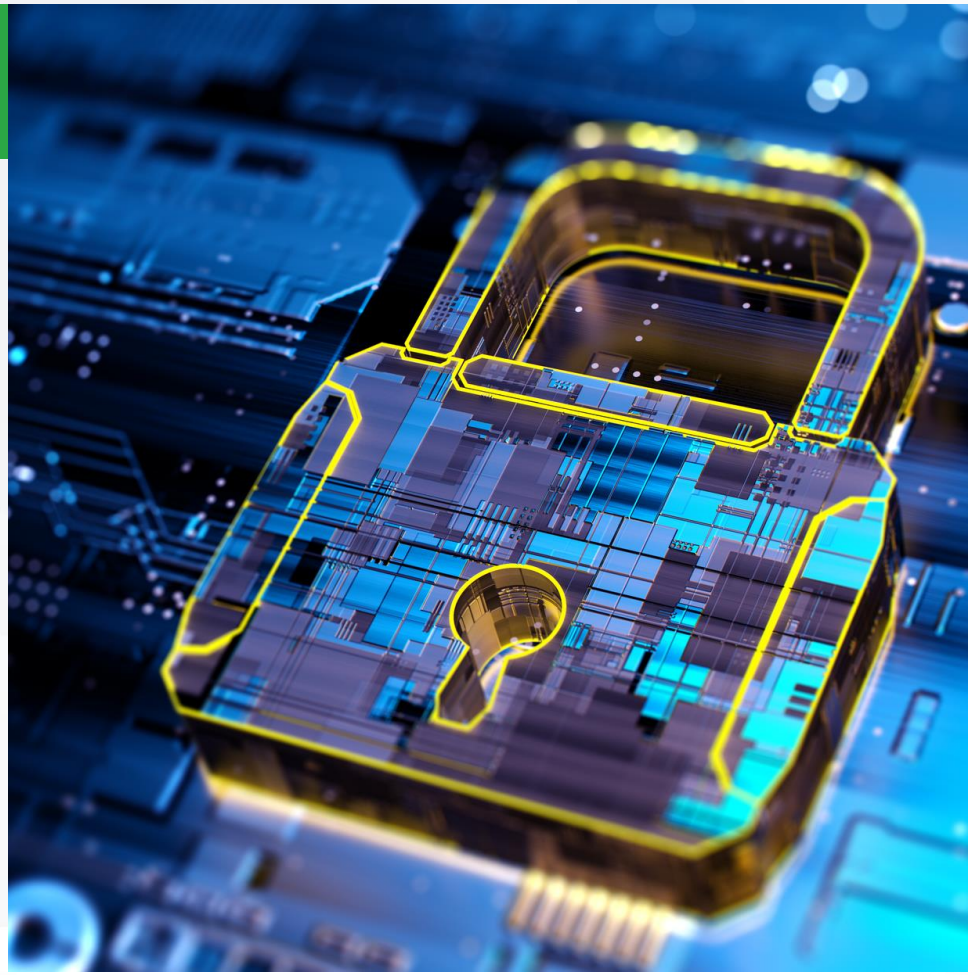
Gestión de claves
Las debilidades o errores en la administración de claves a menudo ofrecen un medio para comprometer un sistema.

Distribución de claves
1. Papel
2. Medios digitales
3. Hardware

Explicación

Aplicaciones y usos criptográficos en la seguridad del sistema de información

- Antimalware.
- Cumplimiento/auditoría.
- Forense.
- Gestión de identificación.
- Propiedad intelectual.
- Proveedores de servicios de seguridad administrados (MSSP).
- Protecciones de mensajería.
- Gestión de parches.
- Defensas perimetrales.
- Información de seguridad y gestión de eventos (SIEM) y respuesta a incidentes.
- Seguridad de transacciones (certificados digitales, transferencia segura de archivos).
- Seguridad inalámbrica.



Actividad

Encripta el siguiente mensaje utilizando el cifrado de transposición simple con una matriz de seis columnas.

Mensaje:

Este es el certificado de Seguridad de Base de Datos

Cierre

La encriptación está conformada por tres conceptos:

Criptografía: arte de escribir en caracteres secretos.

Criptosistema: algoritmos que se utilizan para cifrar y descifrar datos.

Criptoanálisis: proceso de descifrar códigos encriptados.