Seguridad y privacidad

Objetivos

Los objetivos de esta sección sobre seguridad y privacidad son:

1. Comprender los métodos para asegurar la privacidad de la información transmitida.
2. Analizar los diferentes protocolos de cifrado y tecnologías de tunelización.
3. Explorar métodos de ofuscación de datos y algoritmos de cifrado.
4. Estudiar los tipos de fraudes informáticos y robos de información.
5. Investigar la monitorización de redes cableadas e inalámbricas y las amenazas asociadas.

Mapa conceptual

- **Métodos para asegurar la privacidad de la información transmitida**:
    - **Protocolos de cifrado**
    - **Tecnologías de tunelización**
    - **Métodos de ofuscación de datos**
    - **Algoritmos de cifrado**

- **Fraudes informáticos y robos de información**:
    - **Ingeniería social**

- **Monitorización de redes cableadas**:
    - **Conceptos básicos**
    - **Entornos de aplicación**

    - **Herramientas de monitorización**
    - **Amenazas en redes cableadas e inalámbricas**

- **Monitorización de redes inalámbricas**:
    - **Conceptos básicos**
    - **Seguridad en comunicación Wi-Fi**
    - **Herramientas de monitorización**
    - **Amenazas específicas**

Glosario

- **Protocolos de cifrado**: Métodos utilizados para proteger la integridad y confidencialidad de la información durante su transmisión.
- **Tunelización**: Proceso de encapsulación de datos dentro de un protocolo de red para proteger la información transmitida.
- **Ofuscación de datos**: Técnica para dificultar la interpretación de datos mediante su modificación.
- **Algoritmos de cifrado**: Conjunto de reglas matemáticas y operaciones utilizadas para codificar y decodificar datos.
- **Ingeniería social**: Técnica que utiliza la manipulación psicológica para obtener información confidencial.
- **Monitorización de redes**: Proceso de supervisión y análisis de tráfico de red para identificar y responder a amenazas y problemas de rendimiento.
- **Amenazas en redes cableadas e inalámbricas**: Riesgos potenciales que pueden comprometer la seguridad de las redes y los datos transmitidos.

6.1. Introducción

La seguridad y privacidad son pilares fundamentales en el ámbito de la informática, especialmente en la protección de datos sensibles y la prevención de accesos no autorizados.

6.2. Principales métodos para asegurar la privacidad de la información transmitida

Asegurar la privacidad de la información transmitida es crucial para protegerla de accesos no autorizados y garantizar su integridad y confidencialidad.

6.2.1. Protocolos de cifrado

- **Importancia del cifrado**: Protección de datos mediante algoritmos criptográficos durante la transmisión.
- **Tipos de protocolos**: SSL/TLS, IPSec, SSH, entre otros.
- **Implementación**: Configuración adecuada para garantizar la seguridad de las comunicaciones.

6.2.2. Tecnologías de tunelización

- **Definición y uso**: Encapsulación de datos dentro de otro protocolo para proteger la información.
- **VPN (Virtual Private Network)**: Ejemplo de tecnología de tunelización para establecer conexiones seguras a través de redes públicas.

6.2.3. Métodos de ofuscación de datos

- **Propósito**: Dificultar la interpretación de datos

mediante técnicas como el enmascaramiento y la alteración de información sensible.
- **Aplicaciones**: Protección de información crítica durante su almacenamiento y transmisión.

6.2.4. Algoritmos de cifrado

- **Funcionamiento**: Reglas y operaciones matemáticas para cifrar y descifrar datos.
- **Criptografía simétrica y asimétrica**: Diferencias y aplicaciones en la seguridad de datos.

6.3. Fraudes informáticos y robos de información

Los fraudes informáticos y los robos de información son riesgos importantes que enfrentan las organizaciones y usuarios en el entorno digital.

6.3.1. Ingeniería social

- **Definición y técnicas**: Manipulación psicológica para obtener información confidencial de usuarios.
- **Prevención**: Concienciación y formación de usuarios para reconocer y evitar ataques de ingeniería social.

6.4. Monitorización de redes cableadas

La monitorización de redes cableadas es esencial para detectar y responder a amenazas de seguridad y problemas de rendimiento.

6.4.1. Conceptos básicos sobre monitorización de redes cableadas

- **Propósito**: Supervisar el tráfico de red para identificar actividades sospechosas y anomalías.
- **Herramientas de monitorización**: SNMP, Wireshark, entre otras.

6.4.2. Entornos de aplicación de la monitorización de redes cableadas

- **Redes empresariales**: Supervisión de tráfico para asegurar el cumplimiento de políticas de seguridad y rendimiento.

6.4.3. Herramientas de monitorización de redes cableadas

- **Funcionalidades**: Análisis de tráfico, generación de informes y alertas de seguridad.
- **Configuración y mantenimiento**: Implementación adecuada para optimizar la detección de amenazas.

6.4.4. Potenciales amenazas en redes cableadas e inalámbricas

- **Riesgos**: Ataques de denegación de servicio (DoS), sniffing de red, intrusión y explotación de vulnerabilidades.

6.4.5. Ataques a redes cableadas e inalámbricas

- **Tipos de ataques**: Man-in-the-middle (MITM), spoofing, interceptación de datos y ataques de fuerza bruta.

6.5. Monitorización de redes inalámbricas

La monitorización de redes inalámbricas es crucial para asegurar la integridad y seguridad de las comunicaciones Wi-Fi.

6.5.1. Conceptos básicos sobre monitorización de redes inalámbricas

- **Importancia**: Supervisión del tráfico para detectar intrusiones y vulnerabilidades en redes Wi-Fi.
- **Protocolos de seguridad**: WPA2, WPA3 y medidas para proteger redes inalámbricas.

6.5.2. Seguridad en la comunicación inalámbrica Wi-Fi

- **Configuraciones seguras**: Uso de contraseñas fuertes, actualización de firmware y segmentación de redes.

6.5.3. Herramientas de monitorización de redes inalámbricas

- **Funcionalidades**: Detección de dispositivos no

autorizados, análisis de tráfico y detección de patrones anómalos.

6.5.4. Amenazas específicas de redes inalámbricas

- **Vulnerabilidades**: Interferencias, ataques de descifrado de claves, y explotación de debilidades en protocolos de seguridad.