Diseño de redes de computadores seguras (Bastionado de redes y sistemas)

Segmentación de redes

La segmentación de red es una práctica que consiste en dividir las redes en «zonas de seguridad» o segmentos separados por cortafuegos. Cuando se configura correctamente; los segmentos separan las aplicaciones y evitan el acceso a los datos confidenciales.

Subnetting

Una subred es un rango de direcciones lógicas. Cuando una red se vuelve muy grande, conviene dividirla en subredes, por los siguientes motivos: Reducir el tamaño de los dominios de broadcast. Hacer la red más manejable, administrativamente.

Redes virtuales (VLANs)

Acrónimo de virtual LAN, «red de área local virtual», es un método para crear redes lógicas independientes dentro de una misma red física. Dentro de un switch pueden coexistir varias redes virtuales.

Zona desmilitarizada (DMZ)

En seguridad informática, una zona desmilitarizada o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en

Internet.

Seguridad en redes inalámbricas (WPA2, WPA3, etc.)

El problema de las redes WiFi es la seguridad. Existen varias alternativas para garantizar la seguridad de las redes que usan estos estándares.

Consejos que fortalecen la seguridad de las redes inalámbricas:

- Evitar conexiones abiertas.
- Cambiar las contraseñas de acceso.
- Evitar que se pueda tener acceso a través de Internet al router.
- Filtrado de direcciones MAC y direcciones IP.
- Revisar los logs.

Sistemas para proteger las redes inalámbricas:

Wi-Fi Protected Access (WPA), en español «Acceso Wi-Fi protegido», es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).

Una vez finalizado el nuevo estándar 802.11ie se crea el WPA2 basado en este. WPA se podría considerar de «migración», mientras que WPA2 es la versión certificada del estándar de la IEEE.

WPA3 (Wi-Fi Protected Access 3), en español «Acceso Wi-Fi protegido 3», es el sucesor de WPA2 que fue anunciado en enero de 2018, por la Wi-Fi Alliance. El nuevo estándar utiliza cifrado de 128 bits en modo WPA3-Personal (192 bits en WPA3-Enterprise) y confidencialidad de reenvío. El estándar WPA3 también reemplaza el intercambio de claves pre-compartidas con la autenticación simultánea de iguales, lo que

resulta en un intercambio inicial de claves más seguro en modo personal.

Protocolos de red seguros (IPSec, etc.)

Protocolos seguros a nivel de red

Los datos que circulan a través de la red entre aplicaciones son accesibles por terceras personas ajenas a la comunicación, es necesario evitarlo a toda costa mediante el uso de protocolos seguros.

También si importante asegurarse de que los datos no se modifiquen durante el transporte. Los protocolos que aseguran la información a nivel de capa de transporte son SSL y TLS.

El protocolo SSL

Originalmente diseñado por Netscape para establecer comunicaciones seguras con protocolos como HTTP o FTP. Permite negociar qué algoritmos se van a emplear, intercambiar las claves de encriptación y la autentificación de clientes y servidores.

Existen tres versiones del protocolo, la cuarta es una mejora del SSLv3 y se conoce con el nombre de TLS.

El protocolo TLS (Transport Layer Security)

Es una evolución del protocolo SSL (Secure Sockets Layer). La última propuesta de estándar está documentada en la referencia [RFC_2246].

IPsec

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec

también incluye protocolos para el establecimiento de claves de cifrado.

Ejercicios

- **Simular el funcionamiento de una VPN**
  - https://www.jesusninoc.com/01/24/ejercicios-de-seguridad-simular-el-funcionamiento-de-una-vpn-desde-powershell/
- Simular el funcionamiento de un protocolo seguro con Cryptographic Message Syntax (TCP y UDP)
  - https://www.jesusninoc.com/02/11/ejercicios-de-seguridad-realizar-una-comunicacion-tcp-segura-utilizando-cryptographic-message-syntax/
  - https://www.jesusninoc.com/02/11/ejercicios-de-seguridad-realizar-una-comunicacion-udp-segura-utilizando-cryptographic-message-syntax/

Protocolos seguros a nivel de aplicación. SSH

SSH es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.