Implantación de técnicas de acceso remoto. Seguridad perimetral (Seguridad y alta disponibilidad)

Elementos básicos de la seguridad perimetral

La seguridad perimetral corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

Los elementos básicos son:

- Cortafuegos o firewalls.
- Sistemas de detección y prevención de intrusiones (IDS/IDPS).
- Pasarelas «antimalware» y «antispam».
- Redes privadas virtuales (VPN).

Perímetros de red. Zonas desmilitarizadas

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.

Arquitectura débil de subred protegida

Una subred protegida débil es aquella que establece la protección de la red interna empleando una zona DMZ por detrás de un firewall de perímetro.

El equipo que actúa como firewall debe tener al menos tres interfaces para poder conectar con la DMZ, el exterior y la red interna.

Arquitectura fuerte de subred protegida

Arquitectura fuerte de subred protegida. La subred protegida fuerte establece la protección de la red interna con una zona DMZ situada entre dos firewall. En esta disposición el cortafuegos externo (de acceso) bloquea y controla el tráfico no deseado desde la red externa a DMZ.

Redes privadas virtuales. VPN

Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

Beneficios y desventajas con respecto a las líneas dedicadas

Los beneficios de las redes privadas virtuales respecto a las líneas dedicadas son:

- Ahorro de costos en el alquiler de líneas a ISP.
- Escalabilidad.
- Facilidad de manejo en la conexión.

- Proceso transparente para el usuario.
- Los datos viajan encriptados.
- Facilita la movilidad de los usuarios.
- Rapidez en la implementación.

Deventajas:

- Fiabilidad
- Velocidad

Técnicas de cifrado. Clave pública y clave privada

VPN a nivel de red. SSL, IPSec

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/

VPN 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.

Servidores de acceso remoto

Protocolos de autenticación

Algunos de los protocolos de autenticación más comunes son:

- PAP
- CHAP
- TACACS
- RADIUS
- SPAP

Configuración de parámetros de acceso

Los servicios de acceso remoto se crearon en principio para gestionar múltiples llamadas a través de la red telefónica y los modem, por ello, los parámetros de configuración de este servicio son parámetros como puertos de comunicaciones, protocolos de red o sistemas de codificación.

Servidores de autenticación

Un servidor de autenticación es un elemento de la red que controla quién puede acceder a una red informática, por software, por hardware o por una combinación de ambos.