Síntesis conceptual

Grado: Administración de Sistemas Informáticos en Red
Asignatura: Seguridad y alta disponibilidad
Unidad: 3. Seguridad perimetral

Resumen

El término seguridad perimetral hace referencia a la implantación de sistemas de seguridad cuya finalidad es controlar el tráfico que atraviesa la puerta de enlace de una red local hacia el exterior. Este servicio se establece a partir de dispositivos hardware o software entre la LAN e internet: puertas de enlace, cortafuegos o proxies; y esta gateaway o puerta de enlace con el exterior es llama router frontera.

Una DMZ o zona desmilitarizada es una red aislada que se encuentra dentro de la red interna de la organización o empresa donde se destinarán los servicios que requieren de Internet como el correo. Posee entre las redes a las que se conecta cortafuegos. En un entorno más simple o doméstico será el router el que desempeñe esta función de barrera entre equipo e Internet.

Las arquitecturas de seguridad perimetral pueden ser débiles o fuerte:

- La débil: Establece la protección de la red interna empleando una zona DMZ por detrás de un firewall de perímetro.
- La fuerte: Protección de la red interna con una zona DMZ situada entre dos firewalls.

Los sistemas de detección de intrusos, o IDS son herramientas de monitorización que garantizan la continuidad en el tiempo del análisis de los sistemas informáticos y las redes de manera automatizada para detectar ataques maliciosos o intrusos. Existen dos tipos de IDS:

- HIDS (Host IDS): detecta la huella de un atacante, y actúa en consecuencia.
- NIDS (NetworkIDS): analiza las consecuencias de un ataque a partir de las evidencias.

Para evitar ciertos inconvenientes surgen las redes privadas virtuales, VPN, que consisten en crear un "túnel" cifrado por internet entre dos ubicaciones, a través del cual se produce una transferencia de datos similar a la que ocurre en las redes locales, haciendo privada una conexión incluso entre dos equipos a través de la red, al englobar las dos redes de manera transparente. Intentan que dos redes remotas, se convierten en una sola para asegurar el tráfico inalámbrico.

VPN posee múltiples protocolos: PPTP, L2TP/IPsec, SSTP, IKEv2, SSH, Direct Acces y OpenVPN. Algunos de estos protocolos poseen inconvenientes que se pueden solucionar con un segundo cortafuegos.

La elección del protocolo adecuado requiere diversos pasos:

- Antigüedad del servidor y de los equipos.
- Disponibilidad del software VPN.

- Necesidad de disponer el software VPN en los equipos cliente.
- Disponibilidad de certificados digitales válidos.
- Configuración compleja.

Antes de que las VPN fueran creadas, la seguridad empezaba a ser un problema, por lo que se crearon protocolos más seguros como SSH (Secure Shell). Este protocolo permite a cualquier usuario poder conectarse a un equipo de manera remota y segura.

WinRM es un protocolo que emplea servicios web para intercambiar información de administración de servidores.

Escritorio Remoto (RDP) es un protocolo que permite iniciar sesión creando una sesión de escritorio real funcionando de forma similar al igual que si el usuario iniciase sesión de forma física en el nodo al que se conecta. Lo que hace es volcar la información al cliente gráfico, ya que se envía directamente al servidor como si se hubiera generado de forma local, mostrando los resultados en el entorno gráfico.

VNC se trata de un software de control remoto de código abierto. Emplea el protocolo RFB del cual existen varias versiones. Se ejecuta de forma predeterminada en el puerto 5900 TCP y su funcionamiento se basa en colocar datos en forma de píxeles para que toda aquella interacción del usuario se envíe directamente al servidor para ser interpretada posteriormente.

Conceptos fundamentales

- **Tunelización**: acción de encapsular el tráfico de un protocolo.

- **Cortafuegos/firewall**: sistema cuya función es prevenir y proteger a nuestra red privada al bloquear el acceso a cualquier elemento negativo o sospechoso de serlo.

- **Red privada virtual**: conexión entre ordenadores segura basada en la extensión de la red de área local empleando una red pública como Internet.

- **Mainframe**: Computadora especializada y empleada por grandes empresas para el procesamiento masivo de datos.

- **Puerta de enlace**: router que permite que una red enrute su tráfico hacia otra red.