Instituto Universitario de Tecnologia Pascal
Carrera: Informática
Materia: Fundamento de Redes

Redes internas y Externas

Nombre del Estudiante: Yeremi Gonzalez
Número de Estudiante: 04243356112

Introducción

Las redes de área local (LAN) son infraestructuras esenciales en los entornos empresariales y domésticos, ya que permiten la interconexión de dispositivos para la transmisión de datos. Para garantizar su correcto funcionamiento, es fundamental conocer las funciones de enlace de datos, las amenazas a la seguridad en redes internas y externas, los servicios de seguridad disponibles y la importancia del monitoreo en redes TCP/IP. Este trabajo explora estos aspectos clave para comprender mejor la administración y protección de una LAN.

Funciones Principales del Enlace de Datos en una Red LAN

El enlace de datos es la capa 2 del modelo OSI y tiene como objetivo garantizar una comunicación confiable entre dispositivos en una red local. Sus funciones principales incluyen:

- **Encapsulación de datos**: Agrupa los datos en tramas para su transmisión.
- **Direccionamiento MAC**: Usa direcciones físicas para identificar dispositivos en la red.
- **Control de acceso al medio (MAC)**: Regula cómo los dispositivos acceden al medio compartido (Ethernet, Wi-Fi, etc.).
- **Detección y corrección de errores**: Utiliza mecanismos como CRC para verificar la integridad de los datos transmitidos.
- **Control de flujo**: Evita la congestión mediante técnicas como el control de ventana deslizante.

Amenazas en Redes Internas y Externas

Las redes están expuestas a diversas amenazas, tanto internas como externas, que comprometen su seguridad y disponibilidad.

Amenazas Internas

- **Accesos no autorizados**: Usuarios dentro de la red pueden intentar acceder a recursos restringidos.
- **Ataques de ingeniería social**: Manipulación psicológica para obtener credenciales o información sensible.
- **Malware interno**: Dispositivos comprometidos dentro de la LAN pueden propagar virus y troyanos.
- **Errores humanos**: Configuraciones erróneas que exponen la red a vulnerabilidades.

Amenazas Externas

- **Ataques de denegación de servicio (DDoS)**: Sobrecarga de tráfico para inutilizar la red.
- **Intercepción de datos (Sniffing)**: Captura de paquetes en redes no cifradas.
- **Ataques de inyección SQL y explotación de vulnerabilidades web**: Pueden comprometer servidores conectados a la red.
- **Suplantación de identidad (Spoofing)**: Uso de direcciones IP o MAC falsas para acceder a recursos protegidos.

Servicios de Seguridad en Redes

Para mitigar estas amenazas, existen diversos servicios de seguridad que protegen las redes internas y externas:

- **Cifrado de datos**: Protocolos como TLS/SSL y IPsec aseguran la confidencialidad de las comunicaciones.
- **Firewalls**: Filtran el tráfico de red basado en reglas definidas.
- **Sistemas de detección y prevención de intrusos (IDS/IPS)**: Identifican y bloquean ataques en tiempo real.
- **Autenticación multifactor (MFA)**: Aumenta la seguridad en el acceso a sistemas y redes.
- **Segmentación de red**: Divide la LAN en subredes para limitar la propagación de amenazas.
- **VPN (Redes Privadas Virtuales)**: Protegen la comunicación entre redes remotas mediante túneles cifrados.

Monitoreo de Redes TCP/IP

El monitoreo de redes TCP/IP es esencial para garantizar la estabilidad y seguridad de la infraestructura. Algunas técnicas y herramientas clave incluyen:

- **Análisis de tráfico**: Uso de herramientas como Wireshark para examinar paquetes en la red.
- **Supervisión del ancho de banda**: Detecta cuellos de botella y uso anómalo de recursos.
- **Sistemas de gestión de eventos e información de seguridad (SIEM)**: Correlacionan eventos para identificar amenazas en tiempo real.
- **Protocolos de monitoreo**: SNMP (Simple Network Management Protocol) y NetFlow permiten recopilar métricas de rendimiento.
- **Alertas y registros de actividad**: Se configuran sistemas de logging para auditar eventos críticos.

Conclusión

Las redes LAN desempeñan un papel fundamental en la conectividad moderna, pero también enfrentan múltiples desafíos en términos de seguridad y administración. La implementación de mecanismos de enlace de datos eficientes, junto con estrategias de seguridad adecuadas y un monitoreo proactivo de redes TCP/IP, es esencial para mantener la integridad, disponibilidad y confidencialidad de la información. Un enfoque integral en estas áreas permite minimizar riesgos y optimizar el desempeño de la red, asegurando una infraestructura confiable y segura.