Laboratorio: Tarea 4

💡 Jorge Antonio Pérez Ordóñez - 201900810

Diferencias entre las distintas versiones del protocolo VTP

1. **VTPv1 (Versión 1)**:
   - Introducido inicialmente en Cisco IOS 10.0.
   - Proporciona la capacidad de propagar información de VLAN entre switches dentro de un dominio de administración de VLAN.
   - No tiene soporte para la autenticación de mensajes VTP, lo que significa que cualquier switch VTP en el dominio puede enviar actualizaciones de la base de datos VTP sin autenticación.
2. **VTPv2 (Versión 2)**:
   - Introducido para abordar algunas limitaciones y vulnerabilidades encontradas en VTPv1.
   - Introduce soporte para la autenticación de mensajes VTP, lo que permite la seguridad mejorada del protocolo.
   - Se añaden algunas mejoras en la propagación de información de VLAN.
3. **VTPv3 (Versión 3)**:
   - Introducido en versiones más recientes de Cisco IOS.
   - Ofrece mejoras significativas sobre las versiones anteriores.
   - Permite la configuración de múltiples instancias VTP en un solo dominio.
   - Proporciona mayor seguridad y control sobre la propagación de la información de VLAN, incluida la capacidad de filtrar VLAN específicas y configurar revisiones de dominio VTP.

- Permite la distribución de la información de VLAN a través de enlaces troncales seguros.

Diferencias entre los switches de capa 2 y switches de capa 3

1. **Funcionalidad de Capa de Red (Capa 3)**:
   - Un switch de Capa 2 opera principalmente en la Capa 2 del modelo OSI (la capa de enlace de datos), donde se encarga del reenvío de tramas basado en direcciones MAC.
   - Un switch de Capa 3, también conocido como enrutador de Capa 3 o switch de enrutamiento, opera en la Capa 3 del modelo OSI (la capa de red), lo que significa que puede tomar decisiones de enrutamiento basadas en direcciones IP.
2. **Enrutamiento**:
   - Un switch de Capa 2 no puede realizar funciones de enrutamiento de paquetes IP. Simplemente conmuta tramas entre los dispositivos en la misma VLAN.
   - Un switch de Capa 3 es capaz de enrutar paquetes IP entre diferentes redes o subredes utilizando protocolos de enrutamiento como OSPF, EIGRP, RIP, etc.
3. **Funciones de Seguridad**:
   - Los switches de Capa 2 pueden implementar características de seguridad a nivel de VLAN, como VLAN de invitados, autenticación de puerto y Listas de Control de Acceso (ACL) basadas en MAC.
   - Los switches de Capa 3 pueden implementar medidas de seguridad más avanzadas, como ACL basadas en direcciones IP, funciones de firewall, VPNs, etc.
4. **Inter-VLAN Routing**:
   - Para permitir la comunicación entre VLANs, se necesita un dispositivo de Capa 3, como un router o un switch de Capa 3 que admita enrutamiento inter-VLAN.

- Los switches de Capa 3 pueden realizar enrutamiento inter-VLAN directamente en el propio switch, lo que facilita la comunicación entre VLANs sin necesidad de un dispositivo de enrutamiento externo.

Tipos de ataques informáticos a switches de capa 2

1. **Ataque de inundación de tramas (MAC flooding)**:
   - En este tipo de ataque, un atacante envía una gran cantidad de tramas con direcciones MAC falsas al switch. El objetivo es sobrecargar la tabla de direcciones MAC del switch, ya que muchos switches de Capa 2 tienen tablas de direcciones MAC limitadas.
   - Una vez que la tabla de direcciones MAC está llena, el switch entra en un estado de "aprendizaje de direcciones", lo que significa que comienza a retransmitir todas las tramas a todos los puertos, lo que puede facilitar la interceptación de tráfico por parte del atacante.
2. **Ataque de envenenamiento de la tabla de direcciones (ARP poisoning)**:
   - En este ataque, un atacante manipula las tablas de direcciones ARP de los dispositivos en la red enviando falsos mensajes de ARP (Protocolo de Resolución de Direcciones) que mapean direcciones IP a direcciones MAC incorrectas.
   - Cuando un switch de Capa 2 recibe tramas con información de ARP falsificada, actualiza incorrectamente su tabla de direcciones MAC, lo que puede resultar en la redirección de tráfico legítimo hacia el atacante.
3. **Ataque de inundación de broadcast (Broadcast storm)**:
   - En este tipo de ataque, un atacante envía una gran cantidad de tramas de broadcast a la red. Estas tramas de broadcast son retransmitidas por todos los switches en la red, lo que puede generar un tráfico excesivo y provocar una saturación de la red.
   - Como resultado, los recursos de red se agotan y la red puede volverse inutilizable para los usuarios legítimos.