Existen diferentes tipos de ataques a VLAN en las redes conmutadas modernas. La arquitectura VLAN simplifica el mantenimiento de la red y mejora el rendimiento, pero también posibilita el uso indebido. Es importante comprender la metodología general detrás de estos ataques y los métodos principales para mitigarlos.

1. **Los saltos de VLAN** permiten que una VLAN pueda ver el tráfico de otra VLAN. La suplantación de identidad de switch es un tipo de ataque con salto de VLAN que funciona mediante el aprovechamiento de un puerto de enlace troncal mal configurado. De manera predeterminada, los puertos de enlace troncal tienen acceso a todas las VLAN y pasan el tráfico para varias VLAN a través del mismo enlace físico, generalmente entre switches.
2. Los saltos de VLAN permiten que una VLAN pueda ver el tráfico de otra VLAN. La suplantación de identidad de switch es un tipo de ataque con salto de VLAN que funciona mediante el aprovechamiento de un puerto de enlace troncal mal configurado. De manera predeterminada, los puertos de enlace troncal tienen acceso a todas las VLAN y pasan el tráfico para varias VLAN a través del mismo enlace físico, generalmente entre switches

Para prevenir:  inhabilitar los enlaces troncales en todos los puertos, excepto en los que específicamente requieren enlaces troncales. En los puertos de enlace troncal requeridos, inhabilite DTP(Dynamic trunking protocol) y habilite los enlaces troncales manualmente.

1. ataque con salto de VLAN de etiquetado doble (o de encapsulado doble). Este tipo de ataque aprovecha la forma en que funciona el hardware en la mayoría de los switches. La mayoría de los switches realizan solo un nivel de desencapsulación 802.1Q, lo que permite que un atacante incorpore una etiqueta 802.1Q oculta en la trama. Esta etiqueta permite que la trama se reenvíe a una VLAN que la etiqueta 802.1Q original no especificó. Una característica importante del ataque con salto de VLAN de encapsulado doble es que funciona incluso si se inhabilitan los puertos de enlace troncal, ya que, generalmente, un host envía una trama por un segmento que no es un enlace troncal.

Pasos:

1. El atacante envía una trama 802.1Q con doble etiqueta al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal.
2. La trama llega al switch, que observa la primera etiqueta 802.1Q de 4 bytes.
3. El segundo switch observa solo la etiqueta 802.1Q interna que envió el atacante y ve que la trama está destinada a la segunda VLAN

Para prevenir:

para mitigar los ataques de etiquetado doble es asegurar que la VLAN nativa de los puertos de enlace troncal sea distinta de la VLAN de cualquier puerto de usuario.

4) **SPOOFING ATTACK** Estos ataques pueden ocurrir sobre varios protocolos permitiendo a un atacante realizar ataques de man-in-the-middle (MITM), de tal manera que tras el ataque todo el tráfico fluye por el equipo del atacante antes de enviárselo al router, switch o equipo de destino.

Perímetro de PVLAN

segura que no se intercambie tráfico de unidifusión, difusión o multidifusión entre estos puertos del switch

Caracteristicas:

* Los puertos protegidos no reenvían tráfico (de unidifusión, difusión o multidifusión) a ningún otro puerto que también sea un puerto protegido, excepto el tráfico de control. El tráfico de datos no se puede reenviar entre los puertos protegidos en la capa 2.
* El comportamiento de reenvío entre un puerto protegido y un puerto no protegido continúa normalmente.
* Los puertos protegidos se deben configurar manualmente.

Comandos:

**switchport protected** Para configurar la característica de perímetro de PVLAN,

**switchport protected** Para inhabilitar los puertos protegidos.

**show interfaces** Para verificar la configuración de la característica de perímetro de PVLAN