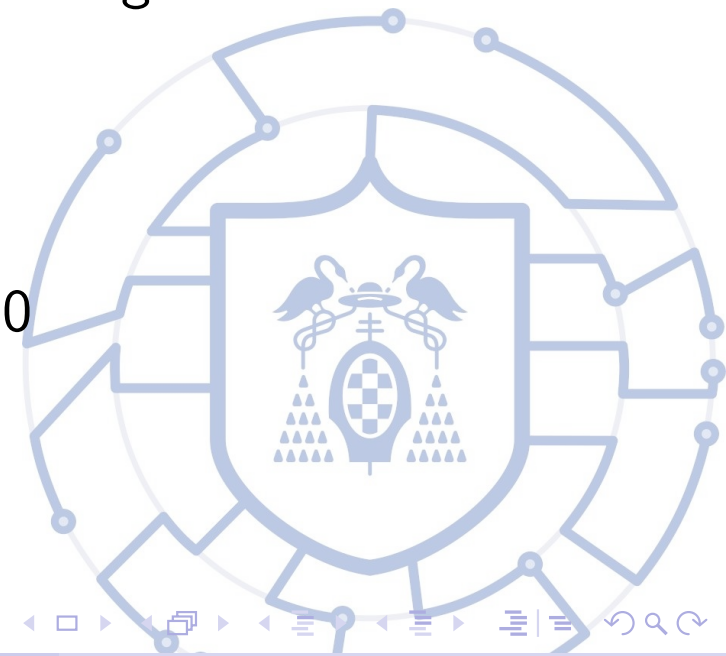
Seguridad en capa de enlace

Ataques y defensas

Daniel López Diego Espinosa Alejandro Rodriguez
Miguel Ortiz Kevin van Liebergen
Marco Santacroce

Universidad de Alcalá

10 de diciembre de 2020



1. Introducción
2. MAC Flooding
3. VLAN hopping
4. Double encapsulation VLAN hopping
5. ARP Spoofing
6. Spanning Tree Attack
7. VLAN Trunking Protocol Attack
8. VMPS/VQP attack
9. Cisco Discovery Protocol attack
10. Private VLAN (PVLAN) attack

¿Qué es VLAN?

Virtual Local Area Network

- Gestionado por un switch
- Separan redes físicas virtualmente
- Limita el alcane de ataques reduciendo el dominio de difusión

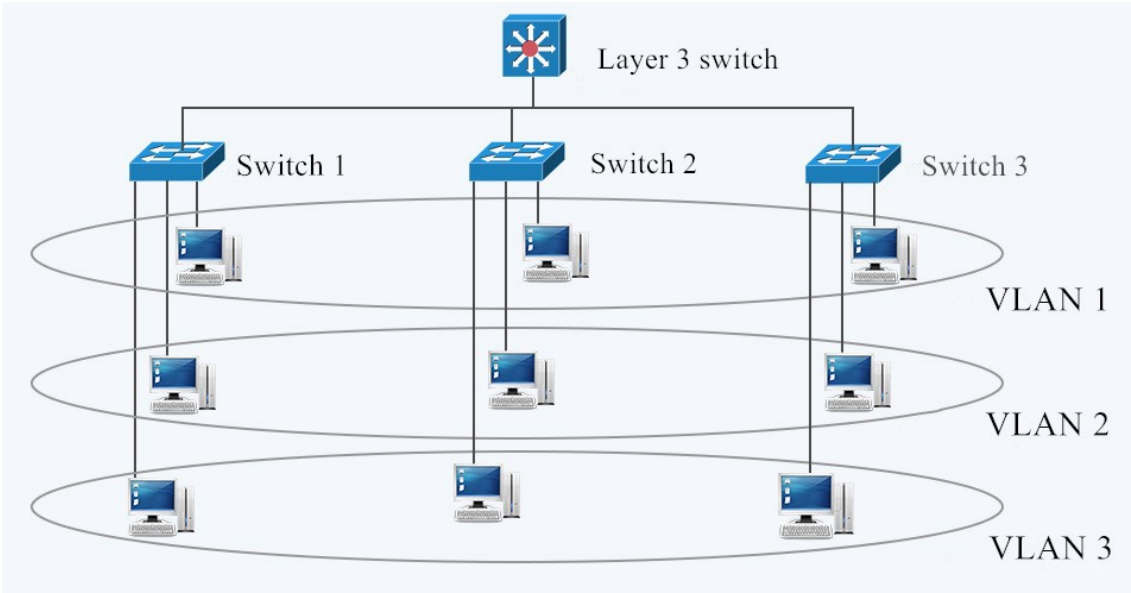


Figura: https://medium.com/

MAC Flooding

- Envío de tramas falsas al switch (falsificando MAC origen)
- El switch agrega entradas falsas hasta que la tabla se llene
- Las entradas con MAC reales se habrán sobreescrito

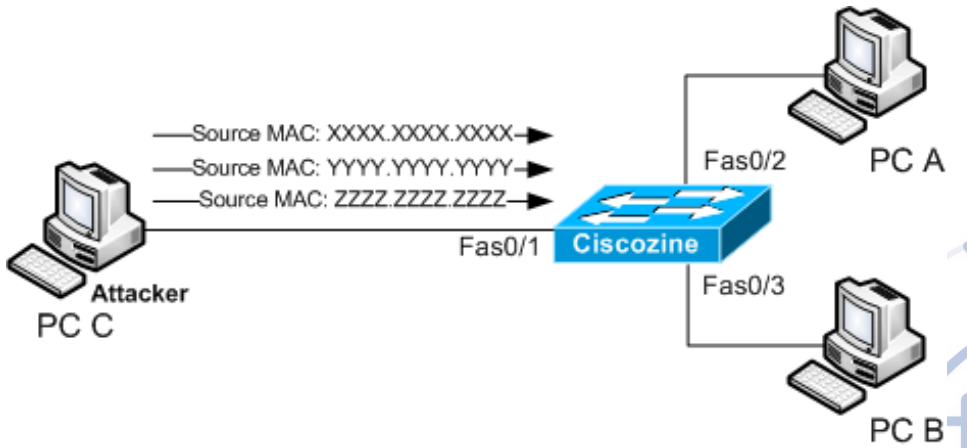


Figura: https://www.ciscozine.com/

MAC Flooding

- Cuando una trama se rediriga, consumirá más ancho de banda y CPU
- Además, el atacante puede capturar dichas tramas

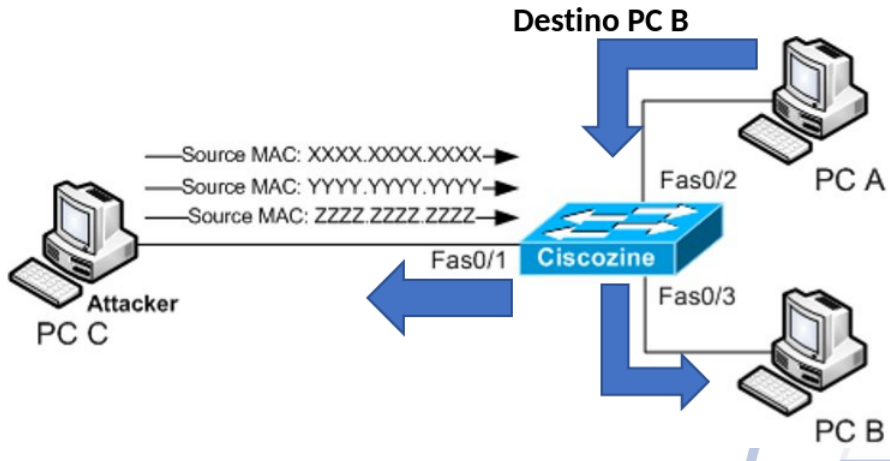


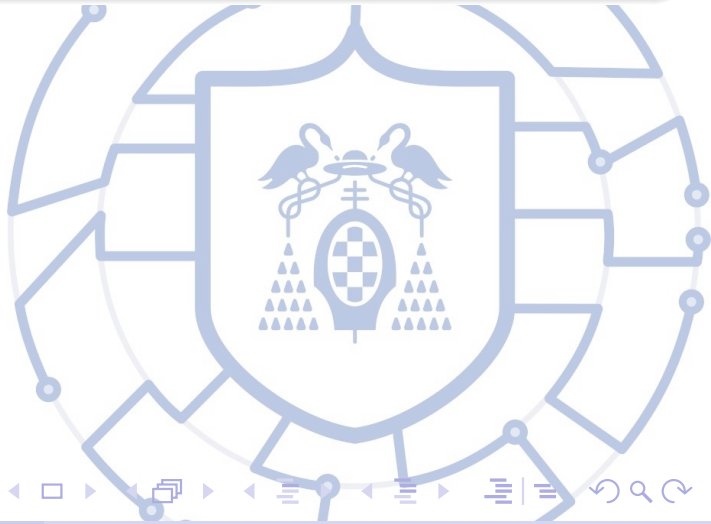
Figura: https://www.ciscozine.com/

MAC Flooding

- Herramientas de ataque: MACOF y DSniff

Solución

Port Security:
Limitar la cantidad de direcciones MAC aprendidas por la interfaz



VLAN hopping

- Un atacante puede implementar DTP (Dynamic Trunking Protocol) y formar un troncal con un swich, de tal forma que tenga presencia en todas las VLANs

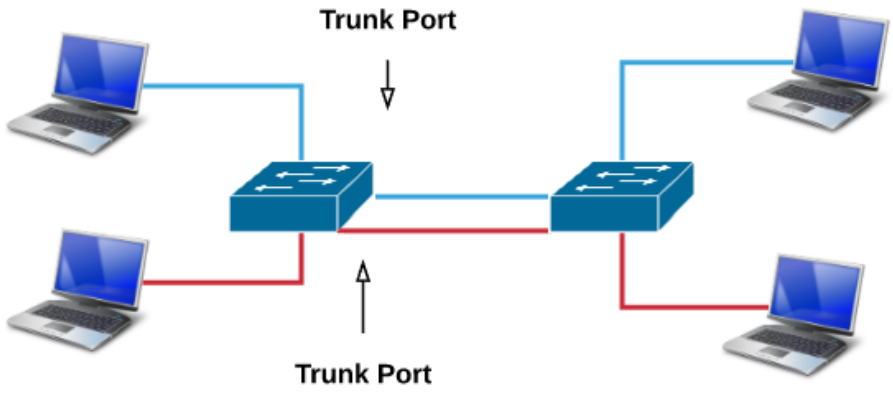


Figura: https://www.oreilly.com/

VLAN hopping

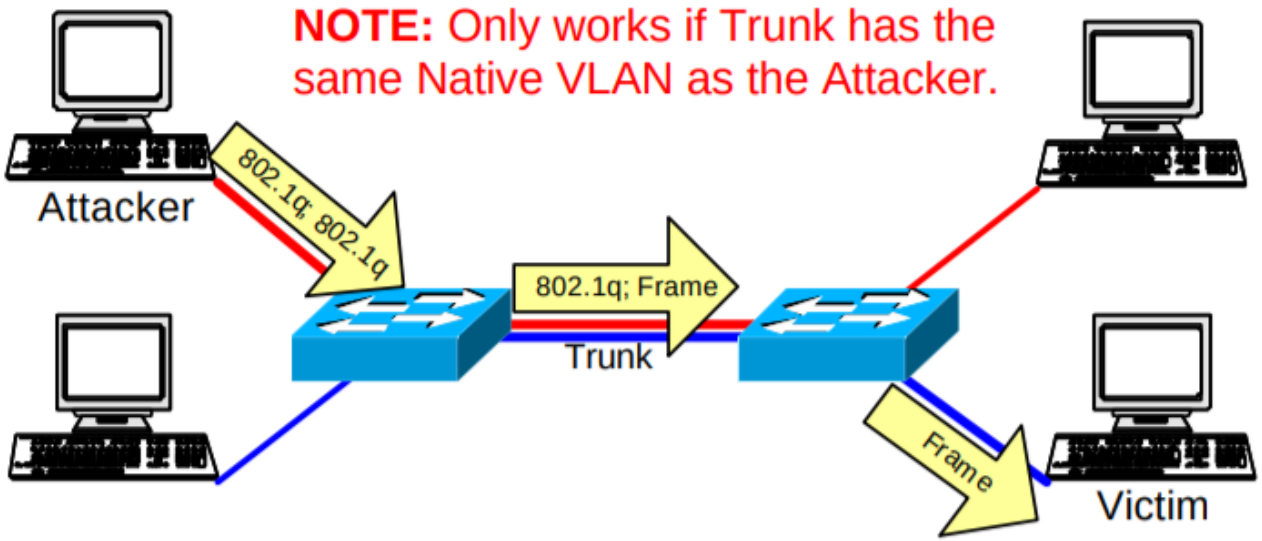
- Herramienta de ataque: Yersinia

Solución

No dejar la configuración por defecto en las interfaces
No implementar DTP en interfaces de acceso

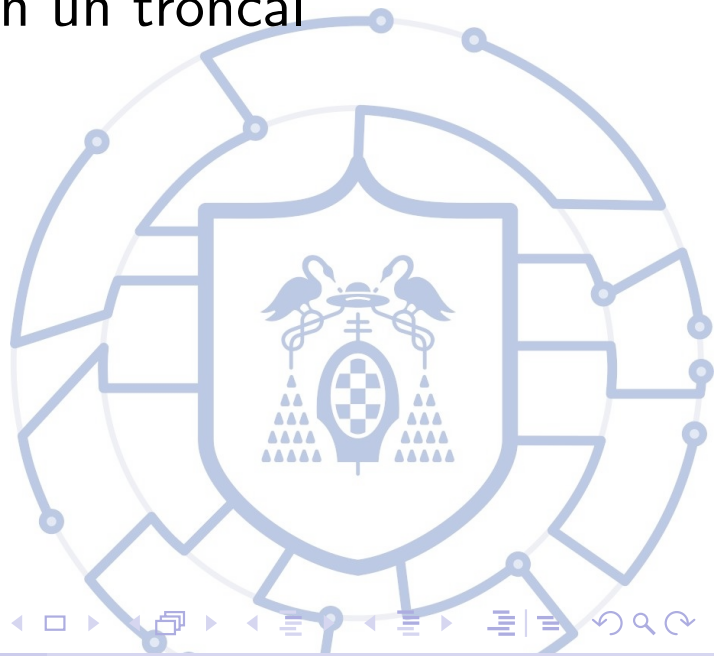
Double encapsulation VLAN hopping

- Variación del ataque VLAN hopping
- Un switch solo puede realizar una operación de desencapsulación



Double encapsulation VLAN hopping

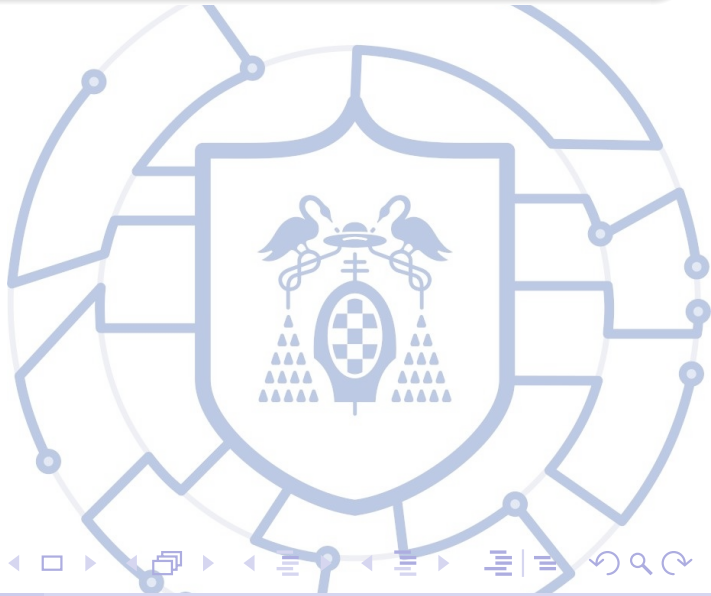
- Un atacante envía una trama etiquetada dos veces
- Utiliza como etiqueta externa la VLAN nativa del troncal
- Los switches no etiquetan la VLAN nativa en un troncal



Double encapsulation VLAN hopping

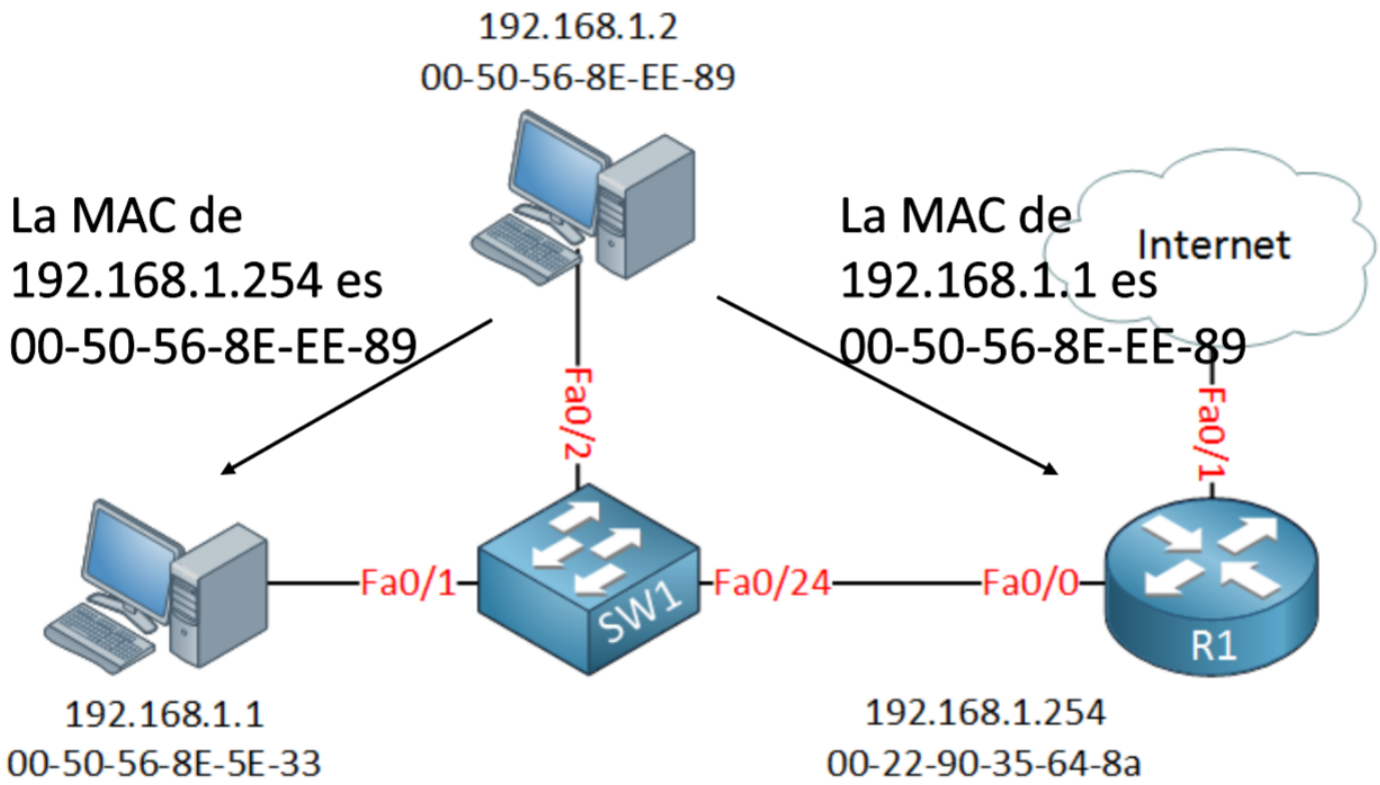
Solución

El administrador debe deshabilitar la opción de Auto-trunking y usar un VLAN ID específico para los puertos truncados



ARP Spoofing

- Manera sencilla de implementar un MiTM
- Comunicación entre la víctima y su puerta de enlace (router) será a través del atacante

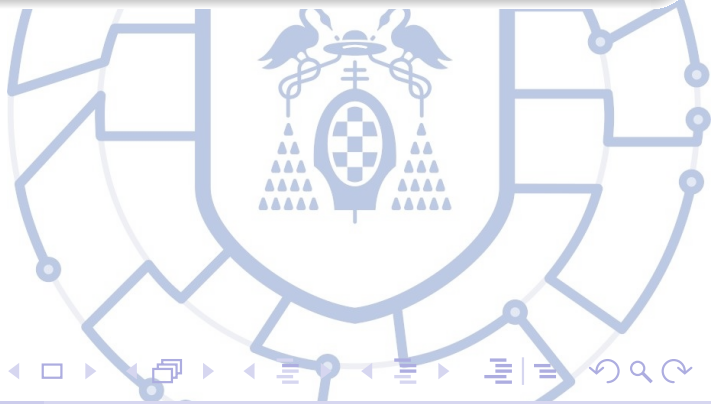


ARP Spoofing

- Herramienta de ataque: Yersinia, DSniff

Solución

Implementar Dynamic ARP Inspection (DAI) en switches de la red
Herramientas de terceros (ARPWatch)
Port Security
IDS



Spanning Tree Attack

- El protocolo STP se utiliza para evitar ciclos redundantes en las topologías de red
- El atacante envía paqutes BPDU a los switches anunciándose como Root Bridge

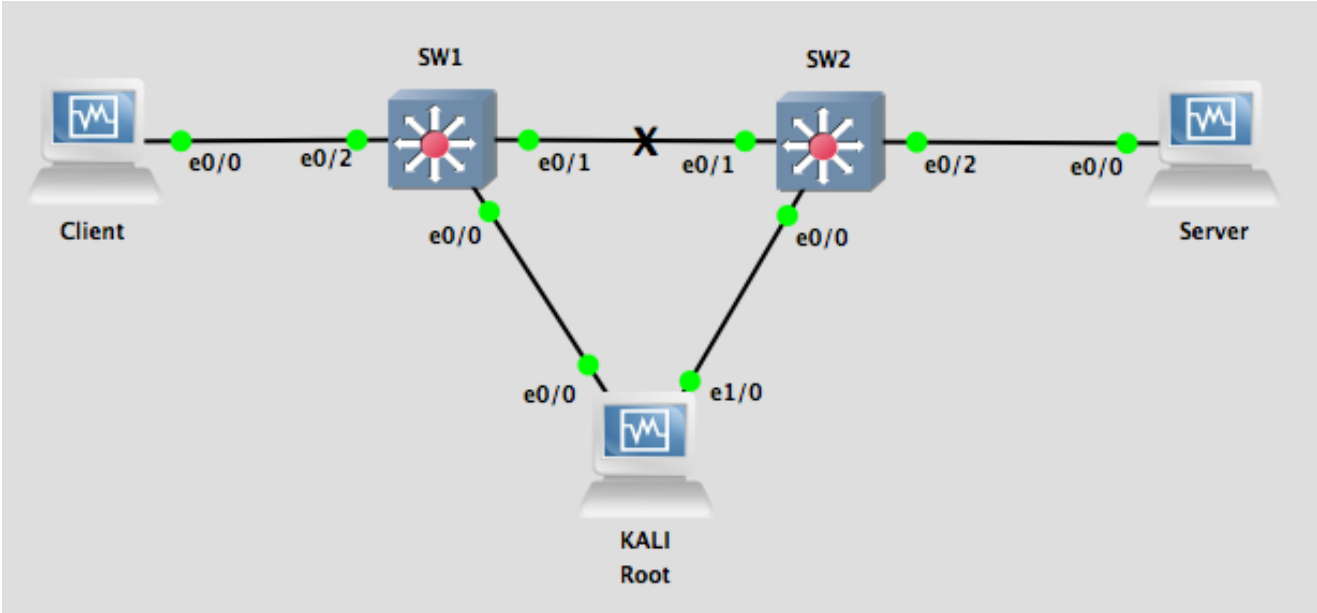


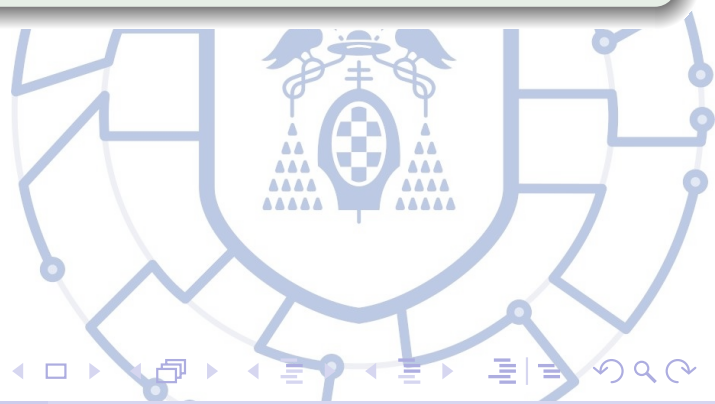
Figura: https://www.jannet.hk/

Spanning Tree Attack

- Fuerza que el tráfico pase por él, pudiendo leer mensaje o causar un DoS.
- Herramientas de ataque: Brconfig y Macof

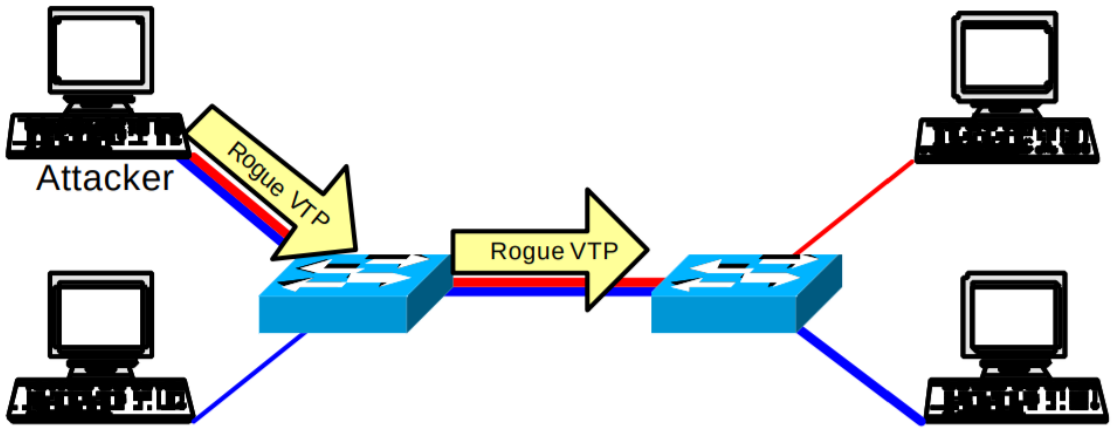
Solución

BPDU Guard: Deshabilitar interfaces que conectan PCs al detectar mensajes BPDU entrantes
Root Guard: Impide que cambie la elección del switch root



VLAN Trunking Protocol Attack

- VTP (Cisco) sirve para extender una VLAN por todos los switches de un dominio
- Si un atacante envía paquetes VTP puede eliminar las VLAN existentes y crear una que estuviera incluido

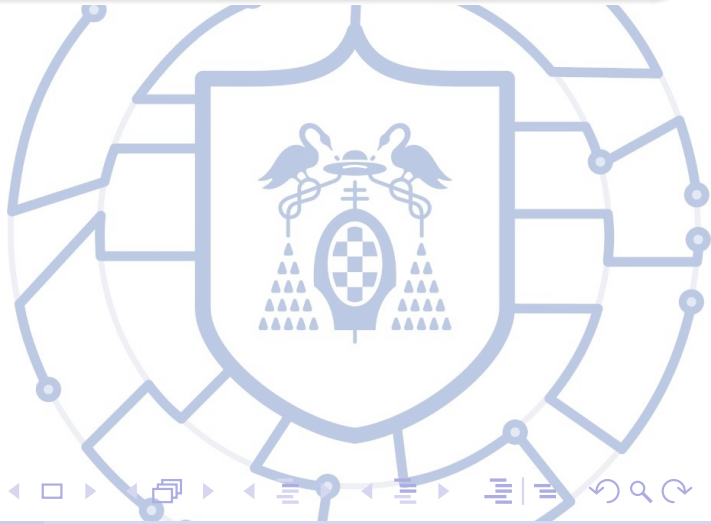


VLAN Trunking Protocol Attack

- Este ataque puede ocurrir por error si se configura mal un switch

Solución

Deshabilitar el uso del protocolo VTP
Si no, utilizar autenticación MD5 en los paquetes VTP

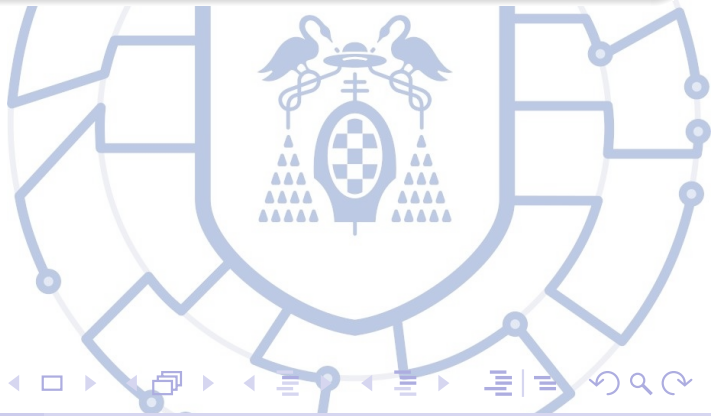


VMPS/VQP attack

- Asignación VLAN mediante VLAN Management Policy Server (VMPS) que utiliza VLAN query Protocol (VQP)
- VQP se encuentra sin autenticar
- Posibles ataques: DoS y suplantación de identidad

Solución

Monitorizar la red y detectar el mensaje VQP



Cisco Discovery Protocol attack

- CDP obtiene información de la red y ayuda a detectar errores
- En claro y sin autenticar
- Un atacante puede hacerse vecino y averiguar la versión del OS y demás información
- Es posible ejecutar un ataque DoS por inundación de mensajes CDP y agotar la RAM de un switch

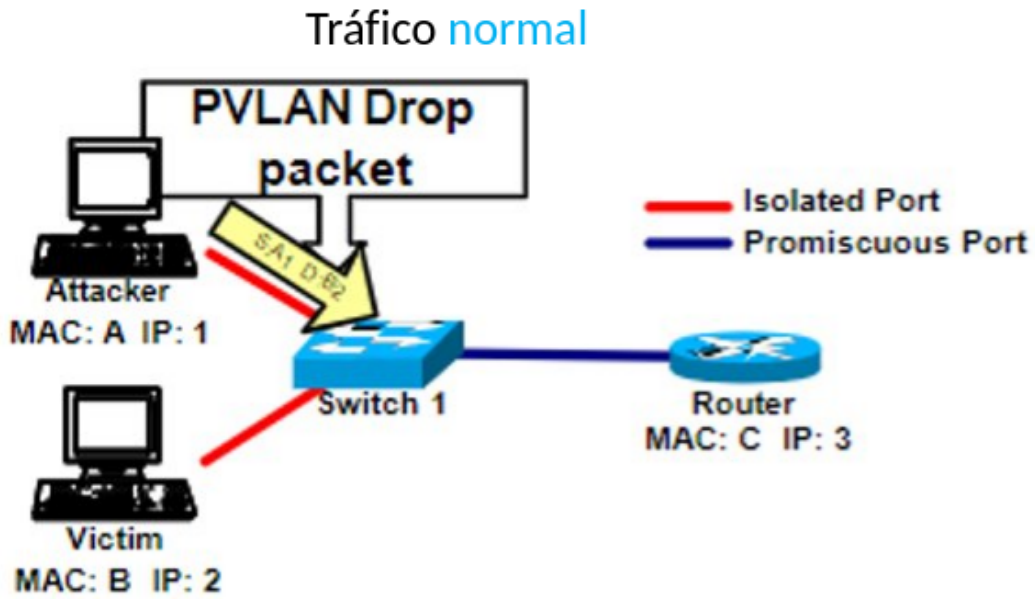
Solución

Deshabilitar CDP

Ser selectivo en nuestros entornos sensibles

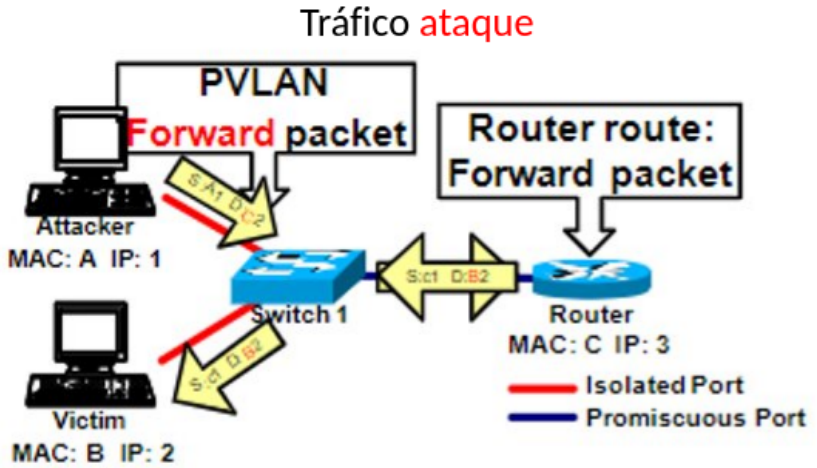
Private VLAN (PVLAN) attack

- Las PVLAN se utilizan para crear redes distintas dentro de una VLAN primaria.
- Una VLAN por puerto en el switch normalmente



Private VLAN (PVLAN) attack

- Mando paquete
  - IP:2 de víctima
  - MAC:C de interfaz switch con enrutador
- El router lo reenvía con la MAC corregida



Solución

Uso de listas de control de acceso

¡Gracias!

¿Preguntas?