

**Tecnológico Nacional de México**

**Instituto Tecnológico de Reynosa**

***Redes VLAN***

***Carrera:*** TICS ***Fecha:*** 29/Ago/22

***Materia:*** Redes emergentes

***Docente:*** Enrique Guerrero Muñiz

***Equipo 4 integrantes:***

19580585 Bermúdez Domínguez Juan Carlos

19580589 Castillo Jr. Gregorio

19580595 Flores Acosta Sheila Lizeth

19580867 Morales Calixto Daniel Alexander

19580603 Góngora Raga Perla Elizabeth

19580633 Pérez Romero Julio Alberto

**Índice**

Índice………………………………………………………………………………………..2

2 redes VLAN…………………………………3

2.1 Tipos VLAN…………………………….7

2.2 Protocolos de enlace VLAN………………………………..17

2.3 Enrutamiento inter VLAN…………………..21

2.4 Resolucion de problemas de VLAN

2.5 Seguridad en VLAN

Bibliografía………………………………………………………………………………..22

**2 Redes VLAN**

**2.1 Tipos de redes VLAN**

**2.2 Protocolos de enlace VLAN**

**2.3 Enrutamiento inter VLAN**

**2.4 Resolución de problema VLAN**

**2.5 Seguridad en VLAN**

Todo buen administrador de redes sabe que seguramente el próximo ataque a sus sistemas provenga de su red. Por malicia o desconocimiento, los usuarios que se encuentran del lado interno tienen mucho más poder destructivo que los externos y eso es así gracias a los administradores confiados.

La red puede ser una de las partes más vulnerables de un sistema. La red de máquinas virtuales necesita tanta protección como una red física. La utilización de VLAN puede mejorar la seguridad de las redes del entorno.

Las VLAN se encuentran en un esquema de redes estándar IEEE, con métodos de etiquetado específicos que permiten el enrutamiento de los paquetes únicamente hacia los puertos que forman parte de la VLAN. Cuando se las configura correctamente, las VLAN constituyen un medio confiable para proteger un conjunto de máquinas virtuales contra intrusiones accidentales o maliciosas.

Las VLAN permiten segmentar una red física de modo que dos máquinas de la red no puedan transmitirse paquetes entre ellas a menos que formen parte de la misma VLAN. Por ejemplo, las transacciones y los registros contables son algunos de los datos internos más confidenciales de una empresa. En una empresa cuyos empleados de los departamentos de ventas, envíos y contabilidad utilizan máquinas virtuales en la misma red física, es posible proteger las máquinas virtuales del departamento contable mediante la configuración de las VLAN.

Empresas de diversos sectores, aseguran sus redes e infraestructuras con la idea de que los ataques siempre vendrán desde el exterior y olvidan que desde dentro de la misma puede sufrir la mayoría de ataques ya sean intencionados o no.

Todo aspecto a recalcar siempre podrá quedarse corto a la hora de tener cubiertas nuestras espaldas dado que con las nuevas tecnologías tanto de ataque como de defensa no podemos tener opciones de quedarnos rezagados a la hora de implementar y de corregir nuestros sistemas.

Asegurar es una opción ineludible, delicada y sobre todo inaplazable porque los ataques pueden producirse de un momento a otro.

Ejemplo de seguridad de VLANs sería que un empleado conecta un SWITCH al cable rj45 que viene asignado a su pc. Así como si estaría activando un servicio DHCP daría direcciones IP a todo nuevo host que se conecte o una conexión WIFI.

***Consejos***

Si configuras una red de área local virtual (VLAN), recuerda que las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales.

* Al usar VLAN, separe los clusters sensibles de sistemas del resto de la red. De esta manera, se reduce la probabilidad de que los usuarios tengan acceso a la información almacenada en esos clientes y servidores.
* Asigne un número de VLAN nativo único a los puertos de enlace troncal.
* Limite las VLAN que se pueden transportar mediante un enlace troncal a las que son estrictamente necesarias.
* Desactive el protocolo de enlace troncal (VTP) de VLAN, si es posible. De lo contrario, configure lo siguiente para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.
* Utilice configuraciones de VLAN estáticas, cuando sea posible.
* Desactive los puertos de conmutador no utilizados y asígneles un número de VLAN que no esté en uso.

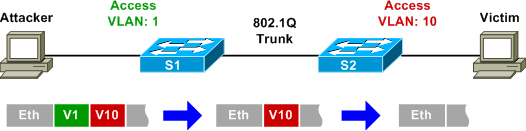
***Tipos de ataques***

***VLAN HOPPING***

Es una vulnerabilidad de seguridad que puede aparecer en entornos LAN, donde los Switch están conectados por puertos troncales.

Un atacante intenta obtener acceso a una VLAN no autorizada mediante la adición de dos etiquetas en los paquetes salientes desde el cliente, esto se llama doble etiquetado. Estas etiquetas se agregan a los paquetes que identifican a qué VLAN pertenecen (VLAN ID).

La primera etiqueta (802.1Q) es leída por el puerto de línea externa en el primer switch al que el cliente-atacante está conectado, donde es eliminada y no se vuele a etiquetar por otra y la envía al siguiente switch, en el segundo troncal se lee la segunda etiqueta que envía tráfico desde el atacante a los clientes con el mismo ID de VLAN como la segunda etiqueta y por ende estos datos serán reenviados.



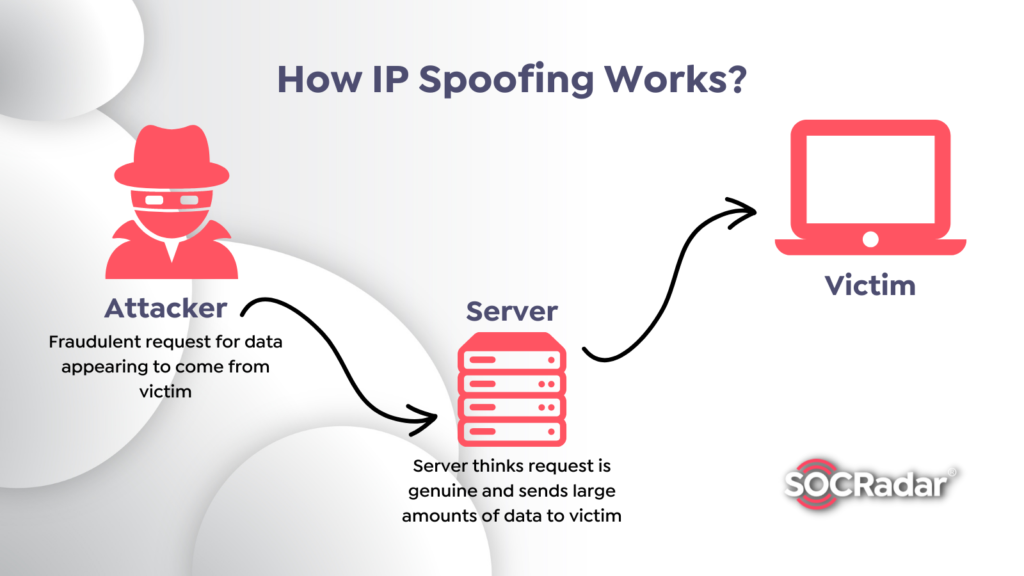
***SPOOFING ATTACK***

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.

Donde el atacante adquiere control y permisos para leer, insertar y modificar las comunicaciones.

El ataque de DHCP Spoofing lo podremos evitar mediante la característica DHCP Snooping de Cisco, mientras que los ataques de ARP Spoofing los podremos evitar mediante las técnicas de inspección dinámica ARP que viene por defecto en los nuevos switches.

Ataques de IP Spoofing los podremos evitar configurando IP Source Guard que uniéndolo a DHCP Snooping el switch conocerá la asociación IP – MAC por puerto, evitando los ataques MitM.



**Bibliografia**

Access Denied. (s. f.). Vmware. Recuperado 3 de septiembre de 2022, de <https://docs.vmware.com/es/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-3887738A-3F3C-4438-B1E7-E35F2A38D94F.html>

Unidad ll. (s. f.). pdf. Recuperado 3 de septiembre de 2022, de <http://www.itpn.mx/recursositics/7semestre/redesemergentes/Unidad%20II.pdf>

Zamorano, J. (2016, 28 marzo). Seguridad en VLANs y sus tipos de ataques. TechClub Tajamar. Recuperado 3 de septiembre de 2022, de <https://techclub.tajamar.es/seguridad-vlans-tipos-ataques/>

Seguridad de VLAN - Sun Blade X4-2B. (2014, 13 agosto). ORACLE. Recuperado 3 de septiembre de 2022, de <https://docs.oracle.com/cd/E50696_01/html/E50091/gmpfo.html>