INSTITUTO TECNOLÓGICO DE SALINA CRUZ

ACTIVIDAD:

INVESTIGACION SOBRE SEGURIDAD VLAN.

DOCENTE:

M.C. SUSANA MÓNICA ROMÁN NÁJERA.

MATERIA:

REDES EMERGENTES.

NOMBRE DEL ALUMNO:

SANCHEZ SANTIAGO NOE.

CARRERA:

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

SEMESTRE: VII. **GRUPO:** "E".

PUERTO DE SALINA CRUZ OAXACA, 4 DE OCTUBRE DEL 2015.

Contenido

INTRODUCCION

Una VLAN de manera muy personal es una subred virtual dentro de una red de área local, permitiéndonos aislar la comunicación de ciertos equipos con otros teniendo un mayor control sobre el tráfico de datos impidiendo que llegue información innecesaria a todos los puertos.

Las LAN virtuales (VLANs) han surgido como una de las soluciones tecnológicas incorporadas en los equipos para redes conmutadas ofrecidos por diversos fabricantes, tanto para aplicaciones de datos y de voz, principalmente IP.

Las razones que justifican el uso de esta tecnología se debe a que ofrecen un mayor control de acceso por parte de los usuario, la red LAN no se ve saturada con tráfico de datos por toda la red, aumentando la productividad en las actividades de los colaboradores de una empresa este aspecto positivo se ve reflejado en mayores ganancias para las organizaciones.

Ahora bien como ya sabemos todo tipo de red requiere que se le establezca seguridad ya que al tratarse de información confidencial o reservada solo para uso de cierta organización se cuida que personas ajenas y mal intencionadas accedan a esta información mediante una vulnerabilidad de nuestra configuración de red.

El objetivo de esta investigación es que se conozca sobre las cuestiones de seguridad que debemos considerar al momento de realizar una configuración y los tipos de problemas de seguridad que suelen presentarse por descuidos o administradores con poca experiencia.

Como ingenieros en tecnologías de la información y comunicaciones es necesario tener conocimientos sobre cómo implementar esta tecnología que nos ofrece grandes beneficios sabiéndola administrar debidamente así como brindar seguridad a la información que transita por esa red e impedir que intrusos nos roben información impactando de manera negativa en la organización que implementa esta tecnología.

ATAQUE DE SUPLANTACION DE IDENTIDAD.

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.

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.

En un ataque de suplantación de identidad de switch básico, el atacante aprovecha el hecho de que la configuración predeterminada del puerto del switch sea dinámica automática. El atacante de la red configura un sistema para suplantar su propia identidad y hacerse pasar por un switch. Esta suplantación de identidad requiere que el atacante de la red pueda emular mensajes 802.1Q y DTP. Al hacerle creer al switch que otro switch intenta crear un enlace troncal, el atacante puede acceder a todas las VLAN permitidas en el puerto de enlace troncal.

La mejor manera de prevenir un ataque de suplantación de identidad de switch básico es 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 y habilite los enlaces troncales manualmente.

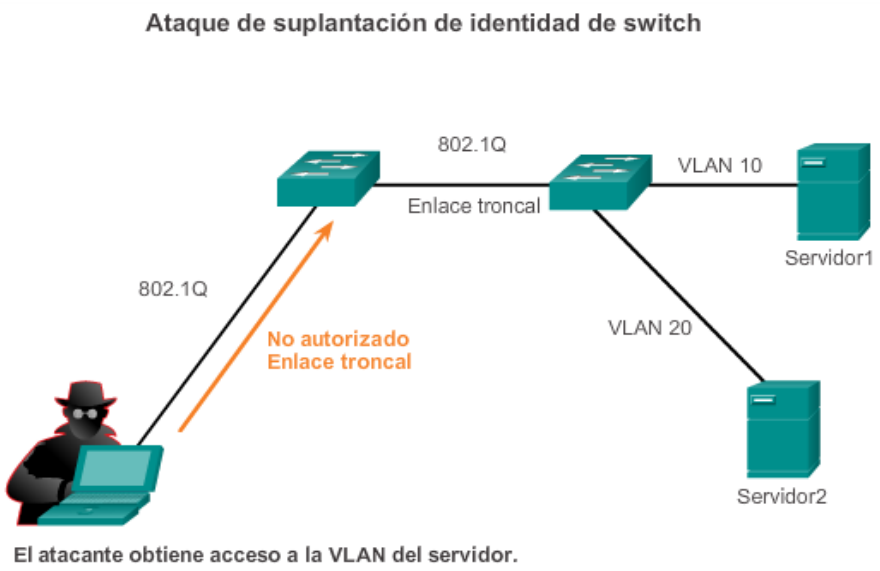

FIGURA 1. EJEMPLO DE SUPLANTACION DE IDENTIDAD.

VLAN DE ETIQUETADO DOBLE.

Otro tipo de ataque VLAN es el 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 des encapsulación 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.

Los ataques con salto de VLAN de etiquetado doble implican los siguientes tres 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. Se supone que el switch procesa la trama que recibe del atacante como si estuviera en un puerto de enlace troncal o un puerto con una VLAN de voz (un switch no debe recibir una trama de Ethernet etiquetada en un puerto de acceso). A los fines de este ejemplo, suponga que la VLAN nativa es la VLAN 10. La etiqueta interna es la VLAN víctima; en este caso, la VLAN 20.

2. La trama llega al switch, que observa la primera etiqueta 802.1Q de 4 bytes. El switch observa que la trama está destinada a la VLAN 10, que es la VLAN nativa. El switch reenvía el paquete por todos los puertos de la VLAN 10 después de eliminar la etiqueta de VLAN 10. En el puerto de enlace troncal, se elimina la etiqueta de VLAN 10, y no se vuelve a etiquetar el paquete porque esta forma parte de la VLAN nativa. En este punto, la etiqueta de VLAN 20 sigue intacta, y el primer switch no la inspeccionó.

3. El segundo switch observa solo la etiqueta 802.1Q interna que envió el atacante y ve que la trama está destinada a la VLAN 20, el objetivo. El segundo switch envía la trama al puerto víctima o lo satura, según si existe una entrada en la tabla de direcciones MAC para el host víctima.

Este tipo de ataque es unidireccional y solo funciona cuando el atacante se conecta a un puerto que reside en la misma VLAN que la VLAN nativa del puerto de enlace troncal. Frustrar este tipo de ataque no es tan fácil como detener ataques de salto de VLAN básicos.

El mejor método 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. De hecho, se considera una práctica recomendada de seguridad la utilización de una VLAN fija distinta de todas las VLAN de usuario como VLAN nativa para todos los enlaces troncales.

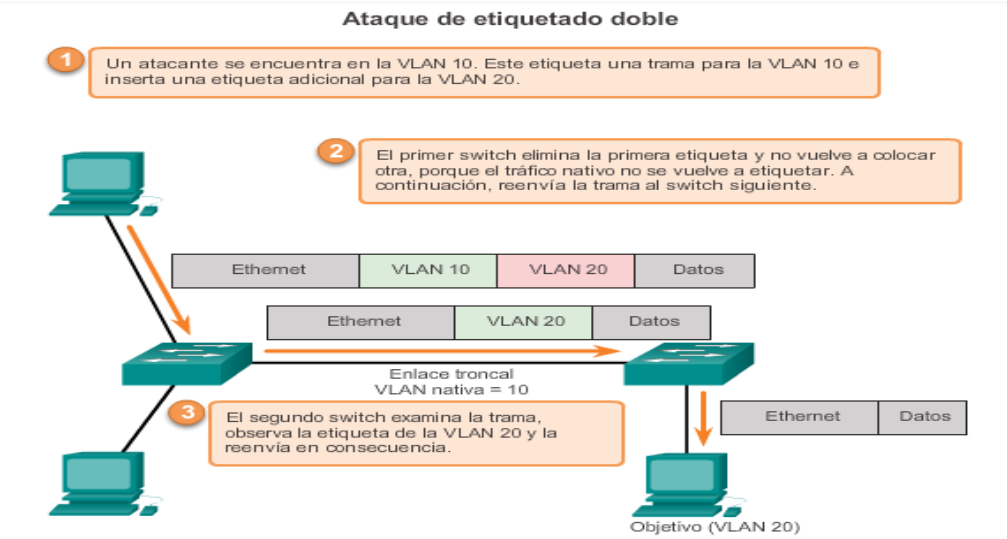

FIGURA 2.ATAQUE DE ETIQUETADO DOBLE.

PVLAN

Algunas aplicaciones requieren que no se reenvíe tráfico en la capa 2 entre los puertos del mismo switch, de modo que un vecino no vea el tráfico generado por otro vecino. En ese entorno, el uso de la característica de perímetro de VLAN privada (PVLAN), también conocida como "puertos protegidos", asegura que no se intercambie tráfico de unidifusión, difusión o multidifusión entre estos puertos del switch.

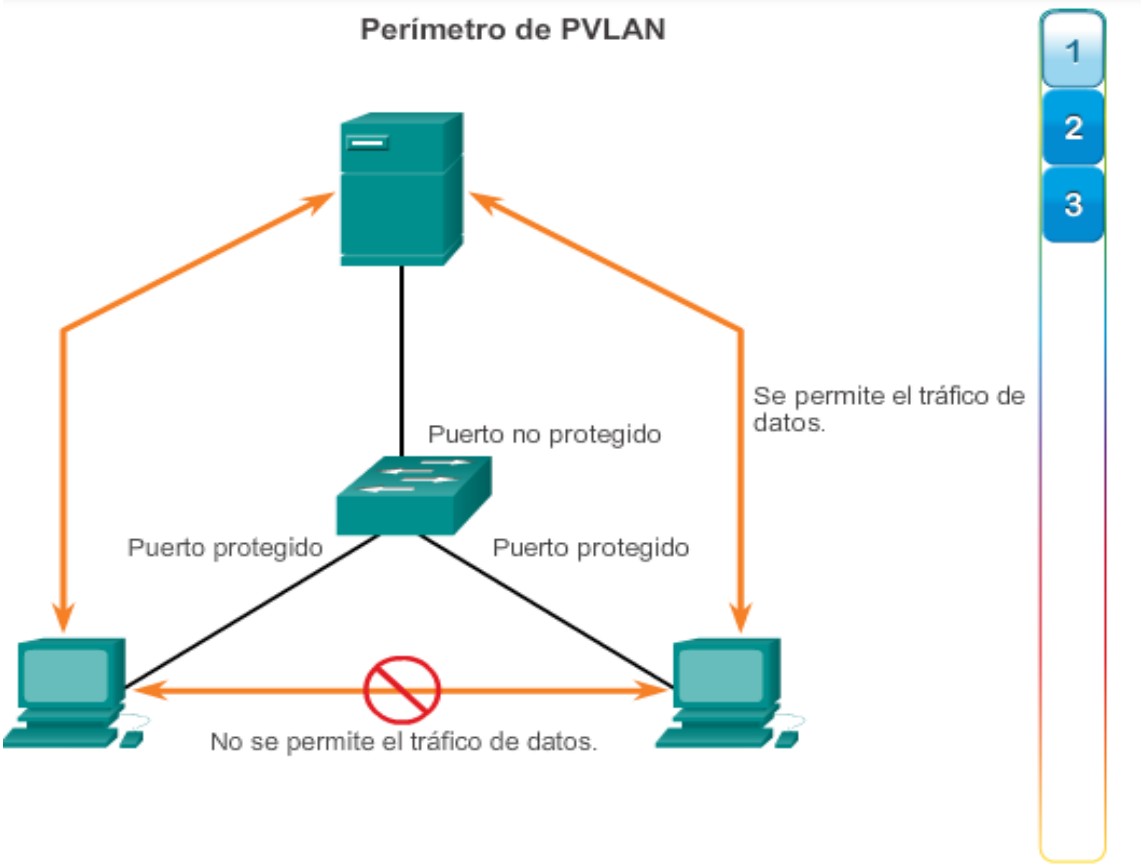

FIGURA 3.PERIMETRO DE PVLAN.

Las características de la función de perímetro de PVLAN son las siguientes:

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. Para

configurar la característica de perímetro de PVLAN, introduzca el comando **switchport protected** en el modo de configuración de interfaz.

```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
 <resultado omitido>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

FIGURA 4. CONFIGURACION DE PVLAN.

Para inhabilitar los puertos protegidos, utilice el comando no switchport protected del modo de configuración de interfaz. Para verificar la configuración de la característica de perímetro de PVLAN, utilice el comando show interfaces id-interfaz switchport del modo de configuración global.

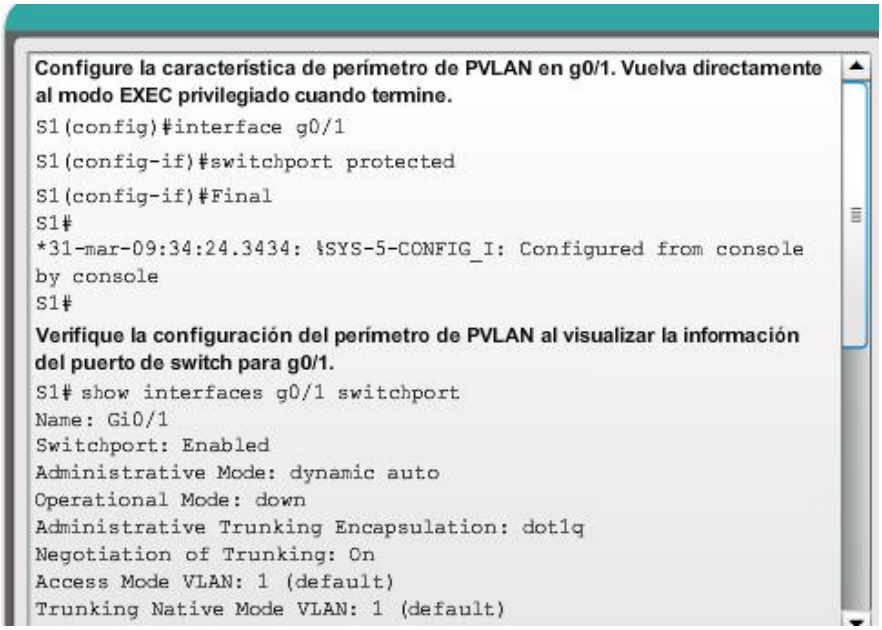

FIGURA 5.VERIFICACION DE CONFIGURACION DE PVLAN PARTE I.

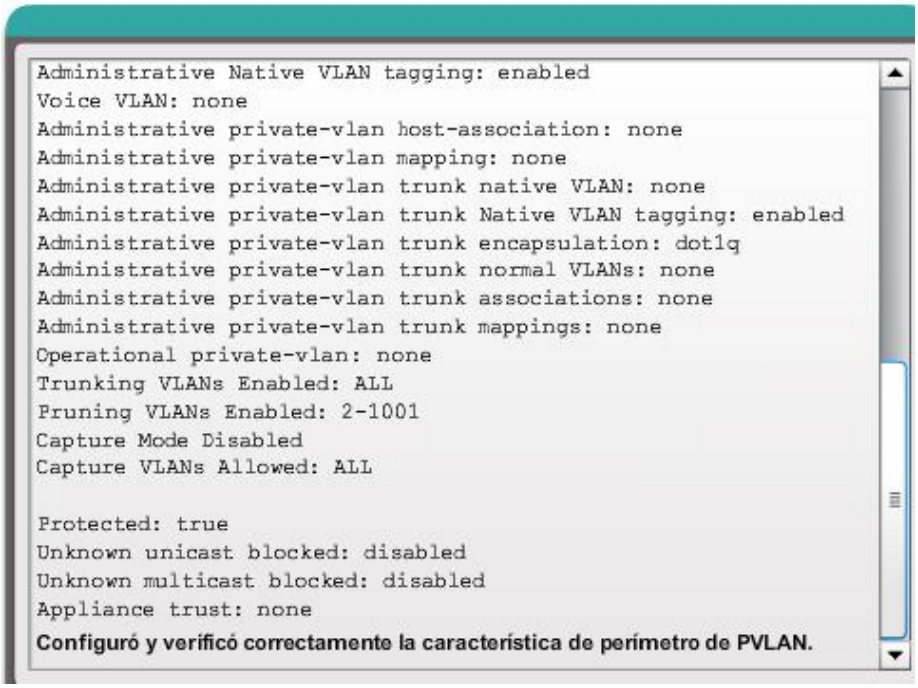

FIGURA 6. VERIFICACION DE CONFIGURACION DE PVLAN PARTE II.

CONCLUSION

Desde un punto muy personal esta actividad de investigación la encontré muy interesante ya que me pude percatar de ciertos aspectos que debo cuidar al momento de hacer la implementación de vlans. Una actividad que ayudo en la comprensión de estos temas fue la realización de una práctica de configuración de seguridad en vlans, de esta manera se logró una buena complementación entre la parte teórica y práctica.

Puedo decir que una medida de seguridad consiste en deshabilitar la negociación automática para evitar que alguien mas conecte un switch a algún otro, ya que si tenemos activada la negociación automática en el momento que se conecte otra extensión a un switch se establece una conexión troncal permitiendo captar información de las otras vlans.

En caso de que algún otro dispositivo llámese computador se conecte a unos de los puertos de un switch que tiene puertos disponibles y el nuevo equipo conectado pertenezca a la vlan 1 o conocida también como vlan por default y de esta manera pueda conocer los datos que transitan por la red con ayuda de alguna aplicación, esta vlan no la podemos eliminar ni modificar es por ello que debemos deshabilitar los puertos restantes de un switch troncal impidiendo que alguien se conecte y pueda acceder a nuestra red sin antes tener una configuración manual por parte del administrador, de esta forma podemos tener un mayor control sobre los usuarios o también podemos realizar configuraciones para que los demás dispositivos pertenecientes a una misma vlan no se enteren de la información que trasmiten los demás equipos lográndose una mayor restricción de la información

Además cabe mencionar que podemos asignar contraseñas a los dispositivos de interconexión para evitar que intrusos puedan hacer nuevas configuraciones ya sea de manera local o remota, en cuanto a seguridad podemos decir que se recurre a muchos métodos de seguridad protegiendo la integridad de la red.

FUENTES CONSULTADAS.

Deivi cesareo. Fleury. Implementación de redes de área local virtuales en un switch. (2007). Fuera de línea. Recuperado el 04 de octubre del 2015 en http://cdigital.uv.mx/bitstream/123456789/31219/1/cesareofleurivicencio.pdf

Richard. Velandia. Protocolo DTP. (2013).Recuperado el 04 de octubre del 2015 en http://networksgoldencross.blogspot.mx/2012/06/protocolo-dtp.html

Roiman. Valbuena. Seguridad en redes de telecomunicaciones e informática. Seguridad VLAN (2008). Recuperado el 04 de octubre del 2015 en http://seguridaddigitalvenezuela.blogspot.mx/2008/08/seguridad-en-redes-vlan.html

Redes cisco. NET. Seguridad en capa 2 VLAN privadas. (2011). Recuperado en 04 de octubre del 2015 en http://www.redescisco.net/v2/art/seguridad-en-capa-2-vlan-privadas/

Cisco Networking Academy. Recuperado en octubre de 2015 en http://www.itesa.edu.mx/netacad/switching/course/module3/#3.3.1.1