Security Policies to Mitigate Attacks VLAN Hopping in the Data Link Layer of LA Networks

Article *in* KnE Engineering · December 2018

DOI: 10.18502/keg.v3i9.3649

7 authors, including:

Carmen Mantilla
Escuela Superior Politécnica de Chimborazo
4 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Alberto Arellano
Escuela Superior Politécnica de Chimborazo
8 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Bertha Hidalgo
University of Alabama at Birmingham
81 PUBLICATIONS **1,691** CITATIONS
SEE PROFILE

KnE Engineering

SIIPRIN-CITEGC
Ibero-American Symposium on Computer Programming jointly held with the International Congress on Technology Education and Knowledge Management
Volume 2018

Knowledge E
Engaging minds

Conference Paper

Security Policies to Mitigate Attacks VLAN Hopping in the Data Link Layer of LAN Networks

Políticas de seguridad para mitigar ataques VLAN hopping en la capa de enlace de datos de redes LAN

Norma Pilamunga[1], Carmen Mantilla[2], Alberto Arellano[1], Byron Vaca[2], Pablo Mendez[4], Blanca Hidalgo[1], and Natalia Layedra[3]

[1]Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Panamericana Sur Km 1 1/2 Riobamba, Ecuador
[2]Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Grupo de Investigación en Seguridad Telemática (SEGINTE), Panamericana Sur Km 1 ½ Riobamba, Ecuador
[3]Escuela Superior Politécnica de Chimborazo, Facultad de Mecánica, Panamericana Sur Km 1 ½ Riobamba, Ecuador
[4]Universidad Nacional de Chimborazo Facultad de Ciencias Políticas y Administrativas, Riobamba, Ecuador

Corresponding Author:
Norma Pilamunga
nopia_ec@live.com

Received: 4 December 2018
Accepted: 5 December 2018
Published: 27 December 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the SIIPRIN-CITEGC Conference Committee.

Abstract

A proposal of security policies based on the ISO 27002 standard is presented, which allows to mitigate VLAN HOPPING attacks at the data link layer level in LAN networks, as it is evident that network administrators pay more attention to policies to ensure the layers of the OSI model, so that internal users with certain privileges can take advantage of these vulnerabilities to access valuable information of the organization. For this purpose, a base network infrastructure of the companies in the city of Riobamba-Ecuador was determined as a case study. In this scenario, a standard four-phase Pentesting was performed to test VLAN HOPPING attacks (Switch Spoofing and Double Tagging) before and after applying the proposed policies, resulting in a 100% mitigation of the technological vulnerabilities found and 90% of organizational, operational, and physical vulnerabilities.

Resumen

Se presenta una propuesta de políticas de seguridad basadas en la normativa ISO 27002 que permiten mitigar los ataques VLAN HOPPING a nivel de capa de enlace de datos en redes LAN, pues se evidencia que los administradores de red ponen mayor atención en políticas para asegurar las capas superiores del modelo OSI, por lo que usuarios internos con ciertos privilegios pueden aprovechar estas vulnerabilidades para acceder a información valiosa de la organización. Para este propósito se determinó una infraestructura de red base de las empresas de la ciudad de Riobamba-Ecuador como caso de estudio, en este escenario se realizó un Pentesting estándar de cuatro fases para probar ataques VLAN HOPPING (Switch Spoofing y Double Tagging)

antes y después de aplicar las políticas propuestas obteniendo como resultado una mitigación del 100% de las vulnerabilidades tecnológicas encontradas y un 90% de las vulnerabilidades organizaciones, operacionales y físicas.

Keywords: VLAN HOPPING, Security Policies, Vulnerability Mitigation, Security Mechanisms

Palabras clave: VLAN HOPPING, Políticas de seguridad, Mitigación de vulnerabilidades, Mecanismos de seguridad.

1. Introducción

El crecimiento acelerado en el uso de tecnología hace que las organizaciones independientemente de su tamaño o actividad, dependan directamente de su infraestructura de red como parte esencial para el éxito del negocio. El activo más valioso es la información [1], por lo tanto, la implementación de políticas de seguridad para el buen uso y configuración de los recursos tecnológicos es importante. Los ataques que sufren las infraestructuras de red cada día son más frecuentes por lo que se convierten en un área vulnerable, y a pesar de invertir en soluciones de seguridad con altos costos se descuida el aseguramiento básico de los dispositivos a nivel de la capa de enlace de datos, por enfocarse solamente en proteger las capas superiores del modelo OSI [2], dejando huecos de seguridad que pueden ser aprovechados por un atacante que en la mayoría de los casos es alguien al interior de la organización, como lo confirman las cifras del laboratorio de McAfee donde el 80% de los ataques provienen del interior de la red [3].

Para el estudio se consideraron de mayor relevancia los resultados de las investigaciones que se listan a continuación:

La investigación "Análisis de tráfico de datos en la capa de enlace de una red LAN, para la detección de posibles ataques o intrusiones sobre tecnologías Ethernet y Wifi 802.11" de Ochoa [4], se enfoca el análisis para determinar cuan seguro es el tráfico de datos en la Capa de Enlace.

Mejía, Ramírez y Rivera [5], en el trabajo de tesis con el tema "Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones", hace un análisis de los ataques en cada capa y como estos afectan

los procesos, además se realiza un análisis de la prevención, detección y mitigación de las principales vulnerabilidades y ataques centrado en la red de datos de toda la organización.

Marro [6], en la investigación "Ataques a la capa de enlace de datos" basa su estudio en los sistemas de detección de intrusiones donde se proponen algunas medidas destinadas a mitigar el impacto de este tipo de ataques.

Altunbasak [7], enfocan los problemas de seguridad en la capa de enlace de datos que no han recibido mucha atención mientras que los problemas de seguridad de red han sido estudiados y abordados en las capas de aplicación, transporte y de red.

Según el INEC, en la ciudad de Riobamba-Ecuador existen 92 empresas entre medianas y pequeñas que son socios de la Cámara de Industrias de Chimborazo, el estudio presenta una realidad principalmente en una mala configuración de los equipos y/o a los permisos elevados a los usuarios internos comunes, lo que en un ataque les permite tener acceso no autorizado a varios recursos de la empresa, dada esta problemática y que la revisión de trabajos existentes se evidenció que no existen en Ecuador estudios específicos sobre la políticas de seguridad para mitigar las vulnerabilidades de ataques VLAN HOPPING, el objetivo del presente trabajo se centra en creación y/o aplicación de dichas políticas, teniendo como prioridad la aplicación de configuraciones concretas para los equipos de capa 2, además de lineamientos para la seguridad de la información, seguridad relativa a los recursos humanos, controles de acceso, seguridad física del entorno y seguridad en las comunicaciones.

Para la creación de las políticas se tomó como base la Norma ISO: 27002 [8], ya que contiene una guía de controles y recomendaciones en cuanto a seguridad de la información, que pueden ser aplicadas en cualquier tipo de organización, el análisis del caso de estudio se utilizó una metodología de Pentesting en cuatro fases estándar propuesta en [9], y el escenario para el caso de estudio resulto de analizar las empresas públicas y privadas de la ciudad de Riobamba-Ecuador, que cumplan con la condición de poseer una infraestructura de red que cuente con equipos de capa 2 (Switch) configurados con VLAN.

Se aplicaron ataques de VLAN HOPPING (Switch Spoofing y Double Tagging) sobre el escenario de caso de estudio, explotando las vulnerabilidades, luego se aplicó las políticas sugeridas que permitan la seguridad de la red en un sistema formado por los dispositivos de red interconectados, tecnologías y buenas prácticas.

2. Metodología

Las fases de la metodología para realizar Pentesting en sistemas informáticos aplicado, se presentan en el Figura 1 [10].

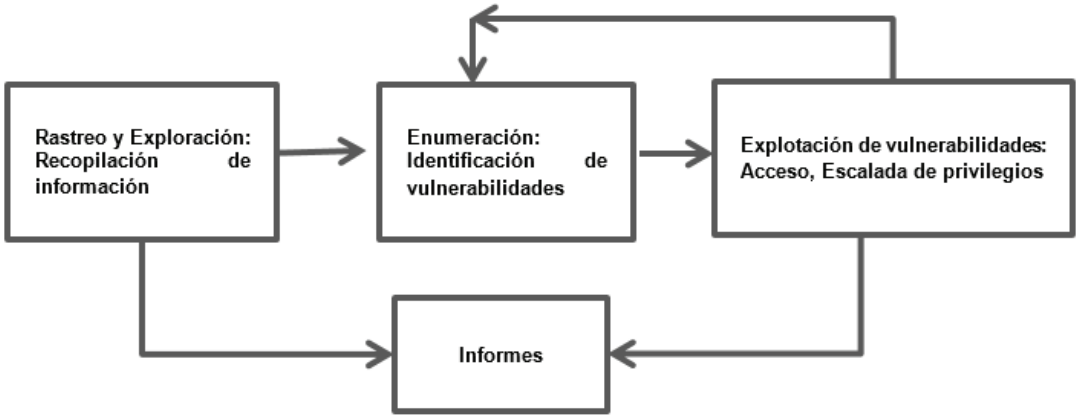

Figura 1: Metodología de Pentesting.

2.1. Fase de Rastreo y Exploración

La recopilación de la información se realizó mediante encuestas y entrevistas a los administradores de red de 30 organizaciones públicas y privadas de pequeño y mediano tamaño de la ciudad Riobamba-Ecuador, ya que cumplen con el parámetro de poseer una infraestructura de red con VLANs y es de donde se derivó el caso de estudio.

2.2. Fase de Enumeración

En esta fase se buscó determinar las vulnerabilidades tecnológicas y operativas, los huecos de seguridad que un atacante como usuario con privilegios y permisos puede aprovechar para tener acceso no autorizado a la red es posible gracias a las potenciales vulnerabilidades tecnológicas causadas debido a una pobre configuración, esto evidenció tras una revisión directa de la configuración de los equipos de capa 2.

Siendo el usuario interno la principal amenaza para vulnerar una infraestructura de red por la incorrecta asignación de privilegios y permisos que tienen dentro de la organización, se deben establecer medidas y normas Organizacionales, Operacionales y Físicas, que ayuden a mitigar ataques VLAN HOPPING.

2.3. Fase de Explotación de Vulnerabilidades

Para la explotación de VLAN Hopping se aplicó los ataques: Switch Spoofing (Suplantación de Switch), donde un atacante configura un equipo para simular que es un switch emulando 802.1Q y señalización DTP [11] y Double Tagging, donde se intenta enviar datos de un switch a otro enviando paquetes con dos encabezados 802.1Q, uno para el switch de la víctima y el otro para el switch de ataque [12]. Se realizaron 10 veces los mismos ataques para descartar fallas en las herramientas utilizadas o fallas humanas.

2.4. Fase de Informes

En esta fase se detallaron las pruebas que se realizaron, se incluyó el listado de fallas y vulnerabilidades descubiertas, además, se presentaron las políticas de seguridad propuestas tanto tecnológicas como organizacionales, operacionales y físicas.

2.5. Caso de estudio

La fase de Rastreo y Exploración definió el escenario de estudio en una configuración estándar de red con equipos de capa 2 y capa 3 CISCO con configuraciones para tecnología VLAN. Para la creación del escenario se utilizó la herramienta de simulación GNS3, ya que permite incluir equipos de diferentes fabricantes y se integra con otras herramientas como VMWARE para virtualizar sistemas operativos Linux y otras plataformas.

La máquina atacante se configuró con Kali Linux, un sistema operativo especializado para realizar pruebas de penetración; los ataques de switch spoofing y double tagging se realizaron con la herramienta Yersinia especializada en ataques a dispositivos capa 2 y se analizó el tráfico con Wireshark.

2.6. Definición de políticas

Una vez realizadas las cuatro etapas de Pentesting y generados los informes finales con los resultados obtenidos, se procedió a la creación de las respectivas políticas de seguridad utilizando como base la normativa ISO: 27002, la aplicación de dichas políticas ayudarán a los administradores de red a mitigar de una manera eficiente los ataques de VLAN Hopping, tanto a nivel tecnológico como organizacional.

3. Resultados

En este apartado se presentan los resultados obtenidos de las pruebas realizadas en la investigación.

3.1. Rastreo y exploración

La Tabla 1., muestra los resultados obtenidos de la encuesta realizada a los administradores de red, como se puede observar la mayoría de las empresas tienen implementadas VLANS. Además como resultado se obtiene que el 66.67 % poseen switchs de marca CISCO, también, se evidencia que a pesar que existe conocimiento sobre ataques de VLAN HOPPING ninguna empresa tiene implementadas políticas ni configuraciones de seguridad en los equipos que ayuden a mitigar este tipo de ataques.

Tabla 1: Resultados de encuesta.

Contexto	Resultado (%)	
	SI	NO
La organización tiene implementados switch en la infraestructura de red	100.00	0.00
El fabricante de los conmutadores que dispone su infraestructura de red es Cisco	66.67	33.33
Los switch de la infraestructura de red son administrables	66.67	33.33
La infraestructura de red tiene implementado VLANs	91.67	8.33
El administrador tiene conocimiento sobre cómo operan los ataques VLAN HOPPING	25.00	75.00
La organización tiene implementado políticas y/o configuraciones de seguridad en relación con ataques VLAN HOPPING	0.00	100.00

3.2. Caso de estudio

En la Figura 2, representa la implementación del escenario de caso de estudio producto de la investigación.

Cuenta con dos switchs de capa 2 y uno de capa 3, configurados con las siguientes especificaciones: se crearon las VLANs 10, 20 y 30, los puertos que se conectan entre switchs están en modo trunk, hay virtual PCs para las diferentes VLANs, la máquina atacante pertenece a la VLAN 10 y trabajó bajo Kali Linux, la máquina víctima pertenece a la VLAN 20 y opera con Centos 6.

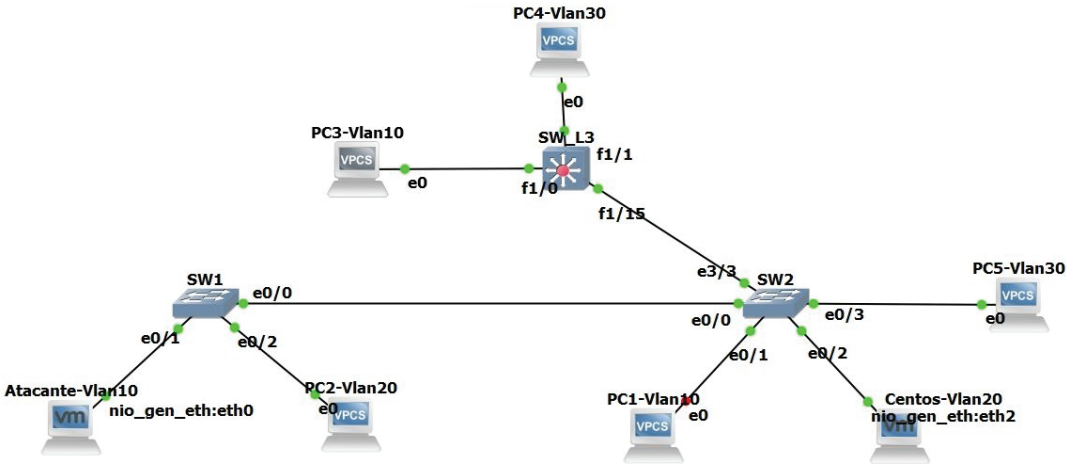

Figura 2: Escenario de caso de estudio.

El escenario contiene todas las funcionalidades y equipos de red que están presentes en las infraestructuras de las diferentes organizaciones encuestadas, las configuraciones y nombres de equipos se realizó de una forma generalizada con el propósito de probar los ataques en un caso no específico.

3.3. Enumeración

Luego de realizar el análisis de vulnerabilidades a los dos switchs de capa 2 en el escenario de caso de estudio, se determina que las principales vulnerabilidades que causan los ataques de VLAN HOPPING (Switch Spoofing y Double Tagging), que son las mismas en los dos casos como se muestra en la Tabla 2., de mayor a menor importancia, la más común y en la que menos se preocupa el administrador es deshabilitar el protocolo DTP que viene habilitado por defecto en los Swtichs CISCO, las demás vulnerabilidades son de igual manera problemas de configuración, pero no vienen por defecto en los Switchs. Las dos últimas vulnerabilidades se consideran dentro de la categoría de organizacionales, operacionales y físicas.

3.4. Explotación de Vulnerabilidades

En la Tabla 3., se resume el número de ataques exitosos y fallidos, realizados a los switchs de capa 2, se puede observar que sus configuraciones permitieron en todos los casos que los ataques tuvieran éxito.

Tabla 2: Vulnerabilidades detectadas.

Vulnerabilidad
DTP habilitado en los switch Cisco por defecto
Configuración automática de los puertos trunk 802.1Q
Uso de la VLAN NATIVA (VLAN 1)
Puertos no configurados en mode "Access"
Puertos sin usar que se encuentran encendidos
Puertos sin uso en VLAN 1
No tienen configurado "VLAN DOT1Q Tag Native"
Usuarios con privilegios y permisos superiores a los que deberían tener
Falta de autentificación a usuarios y equipos, accesos no autorizados

Tabla 3: Prueba de ataques.

Ataque	No. Ataques Exitosos	No. De Ataques Fallidos
Switch Spoofing	10	0
Double Tagging	10	0

3.5. Informes

A forma de resumen las políticas propuestas tanto a nivel tecnológico como a nivel organizacional, operacional y físico para mitigar los ataques de VLAN HOPPING a nivel de capa 2 se presenta en la Tabla 4.

Tabla 4: Políticas de seguridad resultados de las pruebas realizadas.

Políticas de seguridad propuestas	
Tecnológicas	**Organizacionales, Operacionales y Físicas**
No usar VLAN nativa 1 en los puertos trunk.	Políticas de Seguridad de la Información
Colocar los puertos de acceso en modo "Access".	Seguridad relativa a los recursos humanos
Crear una VLAN XY, poner a todos los puertos sin uso a la VLAN XY, declarar estos puertos sin uso en modo "Access"	Control de acceso
Deshabilitar DTP: Nunca dejar un puerto de acceso en modo "Dynamic Desirable ", "Auto Dynamic" o "Trunk".	Seguridad física y del entorno
Apagar todos los puertos no utilizados con el comando shutdown.	Seguridad de las comunicaciones
Etiquetado explícito de la VLAN nativa en todos los puertos trunk. Debe configurarse en todos los switchs de la red.	Gestión de incidentes de seguridad de la información

3.6. Aplicación de políticas

Los resultados obtenidos después de aplicar las políticas propuestas al escenario de caso de estudio, se pueden observar en la Tabla 5., se marcan con SI las vulnerabilidades que se mitigaron después de los dos ataques al aplicar las políticas tecnológicas a la configuración de los switchs, se pueden visualizar en los ítems 1 al 7 y del 8 al 12 se listan las políticas organizacionales, operativas y físicas.

Tabla 5: Resultados de Mitigación de vulnerabilidades al aplicar las políticas.

No.	Vulnerabilidades VLAN HOPPING	¿Se mitigó?	Mitigado (%)
1	DTP habilitado en los switch Cisco por defecto	SI	100
2	Configuración automática de los puertos trunk 802.1Q	SI	100
3	Uso de la VLAN NATIVA (VLAN 1)	SI	100
4	Puertos no configurados mode "Access"	SI	100
5	Puertos sin usar que se encuentran encendidos	SI	100
6	Puertos sin uso en VLAN 1	SI	100
7	No tiene activado "VLAN DOT1Q Tag Native"	SI	100
8	Ausencia de políticas de seguridad	SI	100
9	Usuarios con privilegios y permisos superiores a los que deberían tener	SI	90
10	Falta de autentificación a usuarios y equipos	SI	100
11	Falta de monitorización de la red	SI	90
12	Accesos no autorizados a las instalaciones	SI	90

Es de importancia la implementación en conjunto de las políticas propuestas, para obtener los resultados de mitigación obtenidos ya que al omitir alguna podría dejar un hueco de seguridad no deseado.

4. Conclusiones

Del análisis realizado a la infraestructura de red en las empresas en la ciudad de Riobamba, se encontró que el 100%, no cuentan con configuraciones adecuadas en los equipos de capa 2 para protección de ataques VLAN HOPPING, y a pesar de que en la algunas existen políticas de seguridad normadas en la empresa, estas no son ejecutadas y no están enfocadas a la protección de este tipo de vulnerabilidad.

La aplicación de las políticas de seguridad en el caso de estudio permitió mitigar en un 100% el Ataque Switch Spoofing y en un 100% el Ataque Double Tagging y al ejecutar las políticas organizacionales, operativas y físicas se lograrán reducir y mitigar otro tipo de vulnerabilidades que indirectamente podrían afectar a la infraestructura de reden un 90%.

Las metodologías ISO: 27002 y Pentesting son las más utilizadas a nivel de Latinoamérica y el mundo, estas permitieron tener una referencia de trabajo estándar para facilitar la identificación de vulnerabilidades y la creación de políticas de una organización, que en lo posterior ayudará a reducir el impacto de las vulnerabilidades existentes.

GNS3 y Vmware 11 permitieron simular el caso de estudio, Kali Linux con su herramienta Yersinia hizo posible realizar un análisis completo de vulnerabilidades en equipos de capa 2 para aplicar las correcciones correspondientes y comprobar la efectividad de las soluciones propuestas.

Referencias

[1] Najar, J.: La seguridad de la información: un activo valioso de la organización. Recuperado a partir de https://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/10518/11605. (2015).

[2] Álvarez, W.: Administración de políticas de seguridad en una red de datos bajo una estructura de red definida a través de la utilización del servidor PFSENSE. Universidad Santo Tomás, Bogotá. Recuperado a partir de http://porticus.usantotomas.edu.co:8080/bitstream/11634/714/1/Administracion%20de%20politicas%20de%20seguridad%20en%20una%20red%20de%20datos.pdf (2014)

[3] IMB: Tendencias En Seguridad De Redes: Hacia una protección integral. Recuperado 25 de febrero de 2017, a partir de http://www.emb.cl/gerencia/articulo.mvc?xid=3633&sec=11

[4] Ochoa, V.: Análisis de tráfico de datos en la capa de enlace de una red LAN, para la detección de posibles ataques o intrusiones sobre tecnologías Ethernet y Wifi 802.11. Recuperado a partir de http://repositorio.espe.edu.ec/bitstream/21000/4984/1/T-ESPE-032019.pdf (2011)

[5] Mejía, C., Ramírez, N., River, J.: Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones. Universidad Tecnológica (2015)

[6] Marro, G.: Attacks at the Link Layer. California (2013) 12-14.

[7] Altunbasak, O.: An architectural framework for data link layer security with security inter-layering (2007)

[8] Ges, C.: Controles ISO 27002-2013. Recuperado 9 de marzo de 2017, a partir de http://www.iso27000.es/download/ControlesISO27002-2013.pdf (2013)

[9] Monroy, R.: Evaluación - Test de penetración. Recuperado 20 de mayo de 2017, a partir de https://es.slideshare.net/rodmonroyd/evaluacin-test-de-penetracion (2011)

[10] Díaz, A.: Tests de penetración. Explotación de vulnerabilidades con Metasploit-framework. Recuperado 20 de mayo de 2017, a partir de https://inforensicsuex.wordpress.com/2014/05/14/tests-de-penetracion-explotacion-de-vulnerabilidades-con-metasploit-framework-parte-i/ (2014)

[11] Deivid: Seguridad en VLANs. Recuperado 27 de febrero de 2017, a partir de https://gnulinuxdocs.wordpress.com/2016/08/15/seguridad-en-vlans-ii/?blogsub=confirming#subscribe-blog (2016)

[12] Muñoz, A. Seguridad en redes a nivel de capa 2 (p. 109). Universidad Politécnica de Valencia. Recuperado a partir de https://riunet.upv.es/bitstream/handle/10251/15262/SEGURIDAD{%}20CAPA{%}202{%}20del{%}20modelo{%}20OSI.pdf?sequence=1&isAllowed=n (2011)