ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

POLÍTICAS DE SEGURIDAD PARA MITIGAR LAS VULNERABILIDADES DE LOS ATAQUES VLAN HOPPING A NIVEL DE LA CAPA DE ENLACE DE DATOS EN REDES LAN

NORMA PIEDAD PILAMUNGA AGUALONGO

Trabajo de Titulación Modalidad: Proyecto de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de

MAGISTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

Enero 2019

CERTIFICACIÓN

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación Modalidad**:** El Proyecto de Investigación y Desarrollo, titulado "POLÍTICAS DE SEGURIDAD PARA MITIGAR LAS VULNERABILIDADES DE LOS ATAQUES VLAN HOPPING A NIVEL DE LA CAPA DE ENLACE DE DATOS EN REDES LAN", de responsabilidad de la Srta. Norma Piedad Pilamunga Agualongo ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Juan Mario Vargas Guambo, M. Sc. **PRESIDENTE**	_____ **FIRMA**
Ing. Alberto Arellano Aucancela, Mg. **DIRECTOR**	_____ **FIRMA**
Ing. Blanca Hidalgo Ponce, Mg. **MIEMBRO DEL TRIBUNAL**	_____ **FIRMA**
Ing. Natalia Layedra Larrea, Mg **MIEMBRO DEL TRIBUNAL**	_____ **FIRMA**

Riobamba, Enero 2019

DERECHOS INTELECTUALES

Yo, Norma Piedad Pilamunga Agualongo, con cédula de identidad 020145468-3 soy responsable de las ideas, doctrinas, resultados y propuestas expuestas en la presente investigación y los derechos de autoría pertenecen a la Escuela Superior Politécnica de Chimborazo.

Norma Piedad Pilamunga Agualongo
CI. 0201454683

DECLARACIÓN DE AUTENTICIDAD

Yo, Norma Piedad Pilamunga Agualongo, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor/a, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, 2018

_____

Norma Piedad Pilamunga Agualongo.

C.I.: 0201454683

DEDICATORIA

Este trabajo va dedicado, A mi madre, a mi hermano y hermanas por sus consejos, su compañía y palabras de aliento durante cada etapa emprendida, Al Ing. Diego Avila tutor de esta primera promoción de la Maestría en Seguridad Telemática por ser parte de esta nueva historia profesional, A Carmita, Israel, Luis por su apoyo incondicional, al Ing. Alberto Arellano por su predisposición a ser Director de Tesis, así como también a La Ing. Blanca Hidalgo e Ing. Natalia Layedra por ser miembros.

Norma Piedad

AGRADECIMIENTO

Al único Dios que conquistó mi corazón con su bello amor, que dibuja una sonrisa en mi rostro y hace que toda dificultad se convierta en gozo, valorando cada experiencia para mi existencia, que permite que cada sueño sea cumplido sin siquiera merecerlo, Gracias mil gracias Señor Jesús porque nunca se da por vencido conmigo y me concedido mi petición siendo ya una realidad; porque todo lo imposible para los hombres es posible para Dios.

Norma Piedad

TABLA DE CONTENIDO

INDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

RESUMEN

En este trabajo se implementó políticas de seguridad para mitigar las vulnerabilidades de ataques salto de red de Área Local Virtual (VLAN HOPPING), ya que el estudio evidenció que los administradores de red no prestan atención a la seguridad de dispositivos de Capa de Enlace de datos y la falta de políticas de seguridad adecuadas facilitan varios ataques que puede ser generadas por usuarios internos permitiendo el acceso no autorizado a los recursos y servicios de la infraestructura red. Para esto se aplicó la metodología pentesting en cuatro fases: en la primera fase se recopiló información referente a los equipos de la red; en la segunda se identificó las vulnerabilidades a través del escaneo; en la tercera se explotó en un escenario simulado las vulnerabilidades con el test de intrusión aplicando el ataque suplatanción de switch (Switch Spoofing) que simula ser un switch y el ataque doble etiquetado (Double Tagging) donde el atacante envía datos con dos encabezados 802.Q, las pruebas de penetración se realizaron con la herramienta Yersinia y la cuarta fase donde se realizó un informe donde se detalla las vulnerabilidades descubiertas. Al final se elaboraron políticas de seguridad a nivel tecnológico y organizacional tomando como referencia la ISO 27002 y al aplicarlas se logró mitigar en un 100% las vulnerabilidades VLAN HOPPING, para lograr este resultado es recomendable aplicar las políticas propuestas en conjunto.

Palabras clave: <SEGURIDAD TELEMÁTICA>, <POLÍTICAS DE SEGURIDAD>, <MITIGAR VULNERABILIDADES DE LOS ATAQUES VLAN HOPPING>, <ATAQUES NIVEL DE LA CAPA DE ENLACE DE DATOS EN REDES LAN>, <VLAN HOPPING>

SUMMARY

In this paper, security policies were implemented to mitigate vulnerabilities of virtual local area network attacks (VLAN HOPPING). The study showed that network administrators do not pay attention to the security of data link layer devices. Also, the lack of adequate security policies facilitates several attacks that can be generated by internal users allowing unauthorized access to the resources and services of the network infrastructure. For this, the Pentesting methodology was applied in four phases. In the first phase, information was collected regarding the network equipment. In the second, vulnerabilities were identified through scanning. In the third phase, the vulnerabilities were exploited in a simulated scenario with the intrusion test by applying the switch suplantation attack (Switch Spoofing). That simulates being a switch and the double-tagged attack (Double Tagging) where the attacker sends data with two headers 802Q. The penetration tests were performed with the Yersinia tool. In the fourth phase, a report was made detailing the vulnerabilities discovered. In the end, security policies were drawn up at a technological and organizational level, taking ISO 27002 as a reference and, whit their application VLAN HOPPING vulnerabilities were mitigated 100%. To achieve this result, it is advisable to apply the proposed policies together.

Keywords: <ENGINEERING SCIENCIE TECHNOLOGY>, <TELEMATIC SECURITY>, <SECURITY POLICIES> <MITIGATE VULNERATIES OF VLAN HOPPING ATTACKS>, <NETWORK DATA LINK ATTACKS AT LAN NETWORKS>, <NETWORK SKIP VIRTUAL AREA (VLAN HOPPING)>

CAPÍTULO I

1. MARCO REFERENCIAL

1.1 Introducción

En la actualidad la tecnología está en todos lados, las organizaciones independientemente de su tamaño dependen de su infraestructura de red como parte esencial para el éxito del negocio, donde el activo más valioso es la información por tanto la implementación de seguridades a nivel de hardware y software así como los lineamientos para el buen uso de los recursos son importantes.

Los ataques que sufren las infraestructuras de red cada día son más frecuentes y a pesar de invertir en antivirus, equipos de seguridad con altos costos o monitorear paquetes resultan inútiles ante la pérdida de información.

La LAN (Red de Área Local) sigue siendo el área más vulnerable a los ataques, como lo confirman las cifras del laboratorio de McAfee donde el 80% de los ataques provienen del interior de la red. (Revista, 2015), esto se debe a los privilegios y/o permisos que los usuarios internos tienen para tener el acceso no autorizado a información confidencial.

Se ha evidenciado que el personal técnico descuida el aseguramiento de los dispositivos a nivel de la Capa de Enlace de Datos, por enfocarse sólo a proteger las capas superiores del modelo OSI, dejando huecos de seguridad que pueden ser aprovechados por un atacante, creyendo que la LAN está segura.

Existen técnicas que permiten aprovechar las vulnerabilidades en la LAN como los ataques VLAN HOPPING que facilita el acceso no autorizado a la infraestructura de red, y que una vez que el atacante forma parte de la VLAN (LAN virtual) se convierte en una amenaza activa al haber burlado todas la seguridades y ser capaz de lanzar ataques desde el interior de la red con más probabilidades de éxito.

Hay trabajos revisados que evidencian que no existen estudios específicos sobre Políticas de Seguridad para mitigar las vulnerabilidades de ataques VLAN HOPPING, sin embargo existen aportaciones por separado VLAN SECURITY (Bull, 2015) explica el VLAN HOPPING, Data Link Layer Security Problems and Solutions(Siddique, Ali, & Zubair, 2015), explica cómo explotar la red aprovechando las vulnerabilidades a este nivel, mientras (Sangoluisa, 2015) explica la importancia de definir políticas de seguridad de la información basado en las normas ISO 27000.

Debido a que no se han realizado trabajos que consideren la políticas para mitigar las vulnerabilidades VLAN HOPPING, se presenta este trabajo donde se propone la elaboración de políticas de seguridad adecuadas como prioridad para prevenir o minimizar vulnerabilidades VLAN HOPPING, tomando en cuenta la seguridad de la información, seguridad relativa a los recursos humanos, control de acceso, seguridad física y del entorno, seguridad de las comunicaciones, gestión de incidentes de seguridad de la información y su respectivo cumplimiento, ejecutado en un ambiente de prueba implementada con la topología de red más común en una empresa.

El trabajo está organizado en 5 partes, la primera parte hace referencia al problema localizado a nivel de la Capa de Enlace, la segunda parte contiene la base teórica, la tercera parte se detalla el tipo de investigación, los métodos y las técnicas y los instrumentos a utilizarse para probar la hipótesis. La cuarta parte contiene los resultados de la implementación de las políticas de seguridad aplicado en los escenarios de prueba para finalmente presentar la propuesta.

1.2 Planteamiento del problema

1.2.1 Situación problemática

Esta investigación se origina a raíz del desconocimiento de políticas de seguridad a nivel del usuario interno. Básicamente el crecimiento acelerado del uso de tecnología en las organizaciones, la acentuada dependencia de la LAN, la implementación de tecnologías de seguridad VLAN, las amenazas de seguridad y los hackers hacen que las infraestructuras de red estén propensas a los ataques generados por usuarios internos

que aprovechan la falta de políticas de seguridad para acceder a la información considerada activo de valor.

Conforme a la perspectiva personal, esta investigación presenta una propuesta de POLÍTICAS DE SEGURIDAD PARA MITIGAR LAS VULNERABILIDADES DE LOS ATAQUES VLAN HOPPING A NIVEL DE LA CAPA DE ENLACE DE DATOS EN REDES LAN, que contenga lineamientos necesarios para minimizar el grado significativo de la dimensión de este problema detectado.

1.2.2 Formulación del problema

¿Cómo se mitigan las vulnerabilidades, con la implementación de las Políticas de Seguridad a los ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN?

1.2.3 Sistematización del problema

- Existen pérdidas de la información dentro la organización?
- El personal conoce las medidas de prevención a posibles ataques?
- El personal conoce sobre las políticas de seguridad existentes en su organización?
- Ha existido usuarios sin autorización a las terminales de punto final del personal de la organización
- ¿El administrador de red configura adecuadamente los puertos del switch?

1.3 Justificación de la investigación

La seguridad informática es imprescindible en toda organización, se fundamenta en el establecimiento de controles e implantación de procedimientos y métodos con el objetivo de proteger el activo “la información”. El propósito es proteger la integridad y cumplir con los controles de políticas de seguridad informática.

El uso de redes de área local LAN e infraestructura de seguridad VLAN son ampliamente utilizadas en las organizaciones; pero también existen vulnerabilidades que ponen en peligro la red cuando no hay políticas de seguridad debidamente documentadas, lo que significa que están propensos a los ataques VLAN HOPPING, pero lamentablemente las organizaciones no dan importancia al tema de la seguridad por sus costos operativos.

Los ataques VLAN HOPPING son utilizados para atacar una red enviando paquetes a una VLAN que normalmente no es accesible, para hacer efectivo este ataque se hace uso de dos métodos Switch Spoofing y Double Tagging.

Una de las vulnerabilidades para estos ataques es principalmente el protocolo DTP (Dynamic Trunking Protocol) propio de CISCO que se encarga de negociar el trunking entre switches y de esta manera poder enviar y recibir tráfico entre VLANs.

Por esta razón tener conocimiento sobre los tipos de ataques que afectan a las capas inferiores del Modelo OSI es de interés; el trabajo de investigación DATA LINK LAYER SECURITY PROBLEMS AND SOLUTIONS(Siddique, 2015), explica cómo un atacante puede explotar la red a nivel de la Capa de Enlace de Datos.

Existen trabajos relacionados con los ataques a la Capa de Enlace de Datos, incluso en algunos de ellos se da una breve descripción de los Ataques VLAN HOPPING; pero en el Ecuador y a nivel local específicamente no hay estudios que permitan identificar, analizar, prevenir y mitigar los ataques VLAN HOPPING.

Las redes LAN han crecido en tamaño y en importancia, pero lamentablemente también han proliferado las técnicas de ataque a nivel de Capa de Enlace de Datos, específicamente en los switches que direccionan y controlan el tráfico a través de la LAN, que los convierte en objetivos de los atacantes.

La pobre configuración de los switches por parte de los administradores de red ya sea por descuido, negligencia o desconocimiento crean huecos de seguridad que son aprovechados por los atacantes.

He aquí la importancia de este tema de investigación propuesto de contar con políticas de seguridad adecuadas que pueden ser implementadas por parte del administrador de red en las organizaciones para evitar accesos no deseados de los ataques VLAN HOPPING, protección de la información considerada activo de valor.

1.4 Objetivo General de la Investigación

Implementar Políticas de Seguridad que permita mitigar las vulnerabilidades de los ataques VLAN HOPPING a nivel de la capa de enlace de datos en redes LAN.

1.5 Objetivo Específicos de la Investigación

- Identificar las vulnerabilidades de los ataques VLAN HOPPING.
- Elaborar las políticas de seguridad a implementarse para los ataques
- Elaborar las políticas de seguridad necesarias que contribuya a tener los controles de seguridad informática de la organización.
- Establecer el escenario de pruebas para la puesta en marcha de los ataques VLAN HOPPING.
- Aplicar las políticas de seguridad en el escenario de prueba

1.6 Planteamiento de la hipótesis

¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitiga luego de la aplicación de las Políticas de Seguridad propuestas?

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes del problema

La falta de políticas de seguridad en las redes de área local LAN es un problema que va en aumento, por la desmedida proliferación de herramientas que facilitan los ataques, el incremento del número de atacantes y la desidia por parte de los administradores de red.

VLAN HOPPING es un método para atacar a los recursos en red en una VLAN"(Muñoz, 2011) se logra haciendo uso de los puertos trunk (específicamente enlaces de switch a switch) que permite tener acceso a todas las VLAN. "El término trunk designa una conexión de red que transporta múltiples VLAN identificadas por etiquetas (o tags) insertadas en sus paquetes y que son empleados para transmitir tráfico a través del mismo enlace físico." (Muñoz, 2011)

VLAN HOPPING aprovecha la funcionalidad del protocolo propietario "DTP creado por Cisco Systems y que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet." (Muñoz, 2011).

Sin embargo aun cuando DTP fue creado "para ayudar a los administradores de red en distintas situaciones, si no se cuenta con la experticia necesaria o capacitación son el origen de vulnerabilidades que afectan gravemente el óptimo desempeño de la red interna".(Velandia, 2012) donde los atacantes aprovechan la condición de usuarios con privilegios dentro de la organización.

Las investigaciones realizadas como la de (Baxevanos, 2014) con su trabajo "Protecting with Network Security Strategies a Medium Size Enterprise and Implementing Scenarios Attacks and Countermeasures on Cisco Equipment" presenta las tácticas y métodos de protección de la red local mediante la implementación de medidas de

seguridad, la protección de las comunicaciones y datos. En el trabajo de (Mejía, Ramírez, & Rivera, 2012), hace un análisis de Vulnerabilidades en cada capa del Modelo OSI, tipos de ataques y formas de mitigarlos.

(Bull, Matthews, & Trumbull, 2016) en su artículo pproporciona un listado diferentes categorías de ataque de Capa 2 así como una breve descripción de cada una, posteriormente (Bull, Matthews, & Trumbull, 2016), presenta los resultados de un estudio sistemático para evaluar los efectos del salto de VLAN y los ataques de envenenamiento ARP a través de cinco entornos principales de hipervisor con siete diferentes configuraciones de red virtual.

Finalmente en cuanto a políticas de seguridad se recurre a los trabajos realizados por (Patiño, 2014), (Álvarez, 2014) donde se analiza las vulnerabilidades, amenazas y riesgos existentes en la seguridad informática y se diseña una propuesta de Políticas de Seguridad de la Información.

Con este antecedente, la presente investigación tiene importancia al proponer Políticas de Seguridad para mitigar los ataques VLAN HOPPING, con esto se controlará que los usuarios internos tengan acceso no autorizado a la información y además el administrador de red contará con directrices para realizar una adecuada configuración de los switches, ya que al momento los trabajos de investigación revisados se cubren de manera aislada pues no existe documentación específica referente al título de la investigación.

2.2 Bases teóricas

2.2.1 Modelo OSI

El modelo de interconexión de sistemas abiertos OSI (Open Systems Interconnection) define todos los métodos y protocolos necesarios para conectar una computadora a cualquier otra para formar una red. El modelo OSI es un modelo conceptual que se utiliza con mucha frecuencia para diseñar redes y elaborar la ingeniería de las soluciones de red. (Hallberg, 2007)

El modelo OSI divide los métodos y protocolos necesarios en una conexión de red en siete diferentes capas como se muestra en la Figura 1-2.

Cada capa superior depende de los servicios que ofrece la capa del nivel inferior es un formato que define los métodos y protocolos necesarios en una conexión de red, sus funciones de red se clasifican en siete capas: capa física, capa de enlace de datos, capa de red, capa de transporte, capa de sesión, capa de presentación y capa de aplicación. (Hallberg, 2007)

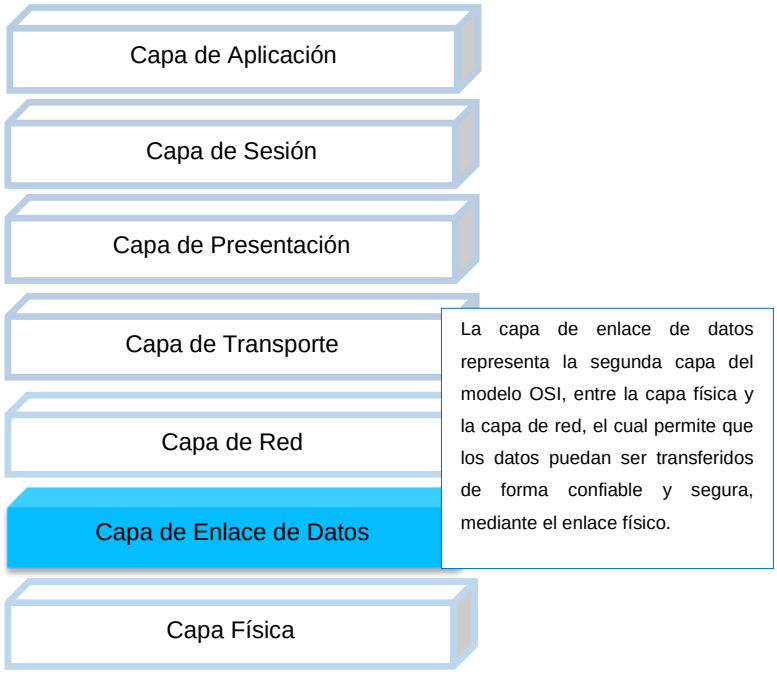


Figura 1-2 Capa de Enlace de Datos

Fuente: Hallberg, 2007

2.2.1.1 *Responsabilidades Modelo OSI*

Cada capa del Modelo OSI tiene responsabilidades como se muestra en la Tabla1-2.

Tabla 1-2 Responsabilidades de las capas – Modelo OSI

7 (Aplicación)	Formato de mensaje en la interfaz de la máquina humana y la visualización de datos.
6 (Presentación)	Encriptación de datos, compresión de datos, conversión de datos.
5 (Sesión)	Sesión establecimiento, mantenimiento y gestión de una sesión.

4 (Transporte)	Control de tráfico de mensajes, aceptación de datos, multiplexación de sesiones, segmentación de mensajes, reconocimiento de mensajes.
3 (Red)	de enrutamiento, control de tráfico de subred, mapeo de dirección lógico-físico, fragmentación de cuadros.
2 (Enlace de Datos)	Establece y termina el lógico entre nodos, reconocimiento de trama, verificación de errores de trama, control de flujo.
1 (Físico)	Bits de transmisión de medios físicos a través de canales de comunicación, codificación de datos, conectividad de hardware físico.

Fuente: (Siddique., 2015)

Elaborado por Pilamunga Norma, 2017

2.2.1.2 *Funcionamiento Capas Modelo OSI*

El modelo OSI nace como una solución a la incompatibilidad de las redes; este modelo por capas o niveles permite que las comunicaciones se organicen en una "pila" de protocolos y que cada capa sea independiente de las demás. Su funcionamiento sería como se muestra en la Figura 2-2.

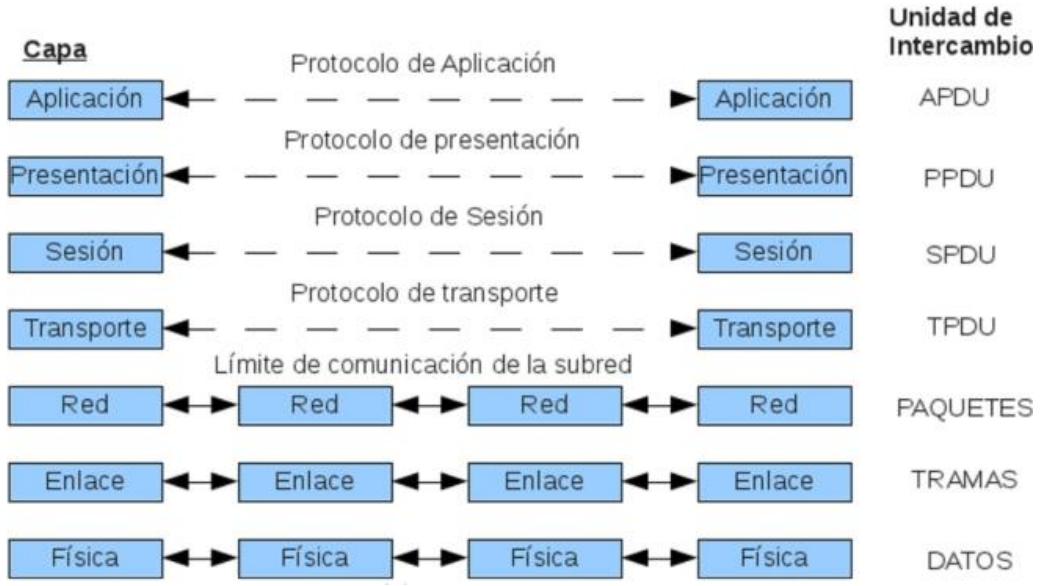


Figura 2-2 Funcionamiento Modelo OSI

Fuente: Muñoz, 2011

2.2.2 Capa de Enlace de Datos

La Capa de Enlace de Datos es la segunda capa del Modelo OSI, transforma la capa física en un enlace de transferencia fiable, es la responsable de la transferencia de información a través de un circuito de trasmisión de datos, como se muestra en la Figura 3-2.

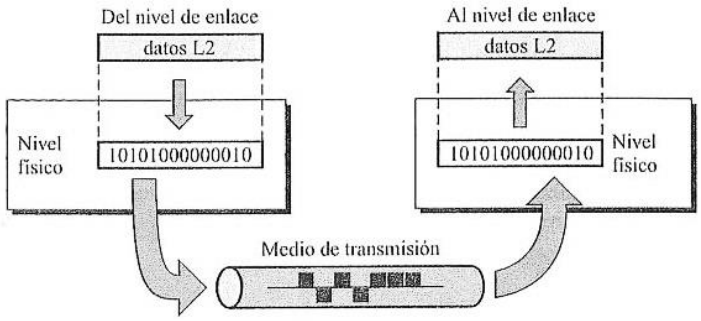


Figura 3-2 Circuito de trasmisión de datos

Fuente: Santos, 2011

Su objetivo es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente. (Tejada, Pérez, & Llibre, 2013). Para lograr este objetivo tiene que:

- Montar bloques de información llamados tramas en este nivel,
- Dotarles de una dirección de nivel de enlace,
- Gestionar la detección o corrección de errores, y
- Ocuparse del control de flujo entre equipos. (Tejada, 2013)

La Capa de Enlace de Datos se divide en dos subcapas como se puede apreciar en el Figura 4-2.

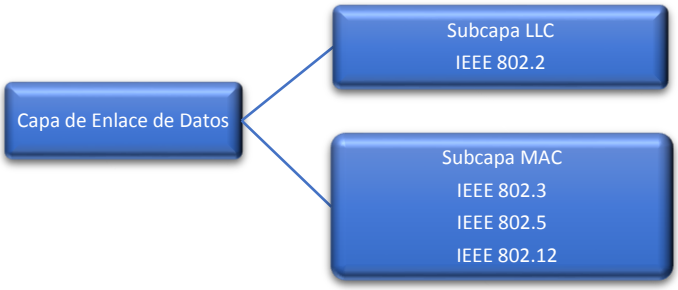


Figura 4-2 Subcapas de la Capa de Enlace de Datos

Fuente: Avalos, 2012

2.2.2.1 *Subcapa LLC*

Coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama.

2.2.2.2 *Subcapa MAC*

El control de acceso al medio MAC es la subcapa de Ethernet inferior de la capa de Enlace de Datos. El hardware implementa, por lo general, el control de acceso al medio en la tarjeta de interfaz de red (NIC).(Ochoa, 2011, p. 66)

Como sabemos en la Subcapa MAC, tiene lugar el **proceso de encapsulación de datos** que incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir la misma. (Ochoa, 2011, p. 70).

"La subcapa MAC se encarga de administrar el control de acceso al medio, esto incluye el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones.

La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor". (Ochoa, 2011, p. 71)

2.2.2.3 *Tramas*

En la Capa de Enlace de Datos, los datos se organizan en unidades llamadas tramas. Cada trama tiene una cabecera que incluye una dirección e información de control y una cola que se usa para la detección de errores.

En este caso la trama es el PDU de la Capa de Enlace de Datos.(Tejada, 2013).

Como podemos observar en la Figura 5-2 la trama se encuentra dividida en encabezado, paquetes (datos) y tráiler.

ENCABEZADO Contiene información de control como direccionamiento y está ubicado al comienzo del PDU				PAQUETES (DATOS) Paquete desde la Capa de red	TRAÍLER Contiene información de control agregada al final del PDU	
Inicio de trama	Dirección	Tipo	Control	DATOS	Detección de errores	Detener trama

Figura 5-2: Trama Ethernet

Fuente: Avalos, 2012

"La trama describe las características requeridas para el transporte de paquetes a través de diferentes medios. Estas características del protocolo están integradas en la encapsulación de la trama. Cuando la trama llega a su destino y el protocolo de capa de enlace de datos saca la trama del medio, la información de tramado es leída y descartada". (Maguana, 2015).

2.2.2.4 *Funciones*

Entre las funciones (Tabla 2-2) de la Capa de Enlace de Datos, tenemos:

Tabla 2-2 Funciones de la Capa de Enlace de Datos

Funciones	Descripción
Armado y separación de tramas	Reconocer y crear los límites de las tramas puesto que la capa física solo reconoce bytes.
Detección de errores	Resuelve problemas de tramas dañadas, repetidas o perdidas.
Control de flujo	Al haber diferencias de rendimiento entre la maquina emisora y la receptora la capa de enlace de datos resuelve problemas de este tipo, regulando el tráfico para que no existan saturaciones o desbordes de memoria
Adecuación para acceso al medio	Se utiliza la MAC (Medium Access Control) la cual es una especie de subcapa que implementa protocolos para controlar el acceso al medio evitando colisiones cuando varias máquinas intentan enviar tramas al mismo tiempo
Creación de Redes LAN Virtuales (VLANs)	En la Capa de Enlace de Datos se crean una serie de redes LAN lógicas que pueden abarcar varias interfaces. Es un método para crear varias redes individuales dentro de una misma red física.
Creación de Puertos Troncales (Trunk):	Los puertos Trunk son puertos por los cuales pasan varias redes distintas en una misma interfaz. Dichos puertos tienen acceso a todas las VLANs de forma predeterminada. Se los emplea para transmitir tráfico de múltiples VLANs a través del mismo enlace físico. La encapsulación puede ser IEEE 802.1Q o ISL.

Fuente: Funciones de la Capa de Enlace de Datos (Mejía, 2012)

Elaborado por Pilamunga Norma, 2017

Como sabemos una VLAN es un método para crear redes lógicamente independientes dentro de una misma red física. Es un grupo flexible de dispositivos que se encuentran en cualquier ubicación de una red de área local.(Capella, 2012). Antes del uso de las VLAN existían varios protocolos propietarios, como el ISL (Inter Switch Link) de Cisco una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com.(Pascal & Petre, 2005)

Porque usar VLAN? Recordemos que los primeros diseños de redes enfrentaron el problema del tamaño de los dominios de colisión (hubs) esto se logró controlar a través del uso de los switches pero a su vez se introdujo el problema del aumento del tamaño de los dominios de difusión y una de las formas más eficientes para manejarlo fue el uso de las VLANs."(Muñoz, 2011)

"Las VLAN funcionan en el nivel 2 (Enlace de Datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red). En el contexto de las VLAN, el término trunk ('troncal') designa una conexión de red que transporta múltiples VLAN identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports ('puertos etiquetados') de dispositivos con soporte de VLAN, por lo que a menudo son enlaces switch a switch o switch a router más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina «canales». Un router (switch de nivel 3) funciona como columna vertebral para el tráfico de red transmitido entre diferentes VLANs." (Muñoz, 2011). Las VLAN se implementan en la capa 2 del modelo de red OSI y su protocolo de etiquetado es IEEE 802.1Q. (Muñoz, 2011)

2.2.2.4.1 *Protocolo 802.1Q*

"El protocolo IEEE 802.1Q es una modificación al estándar de Ethernet. Fue un proyecto del grupo de trabajo 802 de IEEE para desarrollar un mecanismo que permita a múltiples redes conectarse con puentes o switches, compartiendo el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio." (Trunking)." (Capella, 2012)

“El protocolo IEEE 802.1Q permite identificar a una trama como proveniente de un equipo conectado a una red determinada. Una trama perteneciente a una VLAN sólo se va a distribuir a los equipos que pertenezcan a su misma VLAN, de forma que se separan dominios de broadcast.” (Capella, 2012). Esto define el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet como observamos en la Figura 6-2, donde se hace una comparación entre tramas 802.3 y 802.1Q.

802.3	Dirección destino	Dirección fuente	Longitud	DATOS	Relleno	Checksum

	6bytes	6bytes	4bytes	2bytes	46-1500bytes	4bytes
802.1Q	Dirección destino	Dirección origen	Etiqueta IEEE 802.1Q	Longitud	DATOS	FCS

Figura 6-2 Comparación campos de una trama con el protocolo 802.3 y 802.1Q

Fuente: Valdivia, 2015

El protocolo de etiquetado IEEE 802.1Q domina el mundo de las VLAN. El protocolo **IEEE 802.1Q** es una especificación pública. Describe el formato de los paquetes que pasan por enlaces de trunking.

Debido a la naturaleza abierta de la especificación, este estándar se encuentra ahora aceptado por la mayoría de los fabricantes y es la manera común de establecer trunks entre switches de distintos fabricantes. Sin embargo, no es el único protocolo. Algunos fabricantes tienen su propia solución. (Andrés & Barroso, 2009)

Cuándo un switch recibe una trama, añade una etiqueta 802.1Q (4 bytes), recalcula el FCS (Frame Check Sequence) y envía la trama original con las modificaciones por el enlace de trunking.

El campo VID identifica la VLAN a la que pertenece el paquete. Este identificador puede variar entre 0 y 4096. Teóricamente, si hemos establecido el trunking y el switch soporta 802.1Q, podremos enviar paquetes a VLANs distintas. (Andrés & Barroso, 2009)

Para utilizar 802.1Q es obligatorio tener establecido un trunk. Supongamos, entonces, que el enlace de trunk ha sido establecido en el puerto correspondiente. Los ataques contra 802.1Q pueden dividirse en dos clases:

1. Enviar tramas 802.1Q con el fin de enviarlas a VLANs no pertenecientes al atacante,
2. Uso de tramas 802.1Q doblemente encapsuladas – este tipo de ataque añade dos etiquetas al paquete original con el propósito de utilizar la VLAN de la segunda etiqueta como destino, una vez que el switch ha eliminado la primera etiqueta.

ISL es una tecnología propietaria de Cisco, este protocolo guarda información de **VLAN** entre el tráfico de routers y switches, es un método de encapsulación soportado solo en equipos Cisco a través de los enlaces Fast y Gigabit Ethernet. En cierto sentido es una forma compacta de la cabecera del paquete ampliada utilizada en el interior del dispositivo.(Muñoz, 2011)

2.2.2.4.2 *Protocolo DTP (Dynamic Trunking Protocol)*

Protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN con ISL o 802.1Q) en enlaces Ethernet.

Dicho protocolo puede establecer los puertos Ethernet en cinco modos diferentes de trabajo, como se detalla en la Tabla 3-2.(Muñoz, 2011)

Tabla 3-2 Modos de trabajo de los puertos	
Dynamic Auto	Es el modo por defecto en switches Catalyst 2960 de Cisco. El puerto aguardará pasivamente la indicación del otro extremo del enlace para pasar a modo troncal. Para ello envía periódicamente tramas DTP al puerto en el otro lado del enlace indicando que es capaz de establecer un enlace troncal. Esto no quiere decir que lo solicita, sino que sólo lo informa. Si el puerto remoto está configurado en modo on o Dynamic Desirable se establece el enlace troncal correctamente. Sin embargo, si los dos extremos están en modo Dynamic Auto no se establecerá el enlace como

	troncal, sino como acceso, lo que probablemente implique configuración adicional.
On	Suele ser el modo por defecto. Fuerza al enlace a permanecer siempre en modo troncal, aún si el otro extremo no está de acuerdo.
Off	Fuerza al enlace a permanecer siempre en modo de acceso, aún si el otro extremo no está de acuerdo.
Dynamic Desirable	Es el modo por defecto en switches Catalyst 2950 de Cisco. En este modo el puerto activamente intenta convertir el enlace en un enlace troncal. De este modo, si en el otro extremo encuentra un puerto en modo on, Dynamic Auto o Dynamic Desirable pasará a operar en modo troncal.
Nonegotiate	Fuerza siempre al puerto a permanecer en modo troncal, pero no envía tramas DTP. Los vecinos deberán establecer el modo troncal en el enlace de forma manual.

Fuente: Modos de trabajo de los puertos (Muñoz, 2011)

Elaborado por Pilamunga Norma, 2017

Su función es gestionar de forma dinámica la configuración del enlace troncal al conectar dos switches, introduciendo los comandos del IOS (sistema operativo de los switches y routers Cisco) en la configuración del dispositivo (running-config) de forma automática sin que el administrador intervenga. (Muñoz, 2011)

Esto implica que si estamos configurando un puerto de un switch Cisco para DTP, el puerto del otro lado del enlace también debe tener DTP habilitado para que el enlace quede configurado correctamente. (Muñoz, 2011). La combinación de los modos asignados a los puertos define cuál va a ser el estado final del enlace asociado a éstos:

Tabla 4-2 Tipos de Puertos	
Puertos	**Descripción**
Puertos de acceso	Se conectan las estaciones directamente. Mapean el puerto a una VLAN programada. Cuando entra una trama Ethernet se le añade el TAG de 802.1Q. Cuando sale una trama 802.1Q se le quita el TAG, para que llegue a la estación correspondiente con el formato IEEE 802.3 original. Access, es decir, pasarán las

	tramas de una única VLAN y no necesitaremos etiquetarlas
Puertos Trunk:	Se utilizan para conectar Switches entre si y que pase el tráfico de diferentes VLAN a través de ellos. Las tramas que le llegan y que salen llevan el Tag 802.1Q. Trunking es decir, pasarán las tramas de todas las VLAN permitidas etiquetándolas adecuadamente (ISL o 802.1Q)

Fuente: Tipos de Puertos (Muñoz, 2011)

Elaborado por Pilamunga Norma, 2017

La Tabla 5-2 describe las combinaciones de modos y el estado final del puerto al que se llega, asumiendo que ambos lados tienen DTP habilitado:

Tabla 5-2 Modos y combinaciones de los puertos DTP

Puerto	**Modos**			
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Fallo
Access	Access	Access	Fallo	Access

Fuente: Modos y combinaciones de los puertos DTP (Muñoz, 2011)

2.2.2.5 *Ataques Capa de Enlace de Datos*

Hoy en día los ataques en una LAN son más comunes de lo que podríamos imaginar, y es que a través del avance tecnológico la forma de atacar ha mejorado y son capaces de explotar vulnerabilidades en el diseño y configuración de los equipos de la infraestructura de red; por ejemplo uno de los ataques en la Capa de Enlace de Datos, es el VLAN HOPPING que aprovecha la diseños débiles de configuración y al no contar con herramientas para su detección pueden aprovechar estas debilidades lo que significa que el atacante pueda realizar acciones maliciosas dentro de la red LAN.

Por esta razón estos ataques necesitan ser mitigados a nivel de switch, a continuación en la Tabla 6-2 detallamos los ataques que pueden comprometer a la Capa de Enlace de Datos.

Tabla 6-2 Ataques de Capa de Enlace de Datos	
ATAQUES	**DESCRIPCIÓN**
ATAQUES MAC	En este ataque, un conmutador se inunda con numerosas direcciones MAC aleatorias para llenar el búfer de memoria de direcciones de contenido (CAM) dentro del conmutador forzándolo a un modo a prueba de fallos, también conocido como modo de concentrador.
ATAQUES STP	En este tipo de ataque, las tramas de BPDU incorrectas se envían a los conmutadores para modificar la topología del árbol de expansión implementada en la red. Al explotar STP, un atacante podría realizar un ataque de hombre en el medio (MITM) que permite escuchar a escondidas en el tráfico que pasa entre dos nodos en una red
ATAQUES VLAN	Las VLANs se implementan para generar un control de tráfico entre las mismas, de forma que los equipos conectados a una VLAN no posean acceso a otras. Este tipo de ataque pretende engañar a un switch, sobre el cual se implementan VLANs, mediante técnicas que logran conocer los paquetes de información que circulan entre ellas, y como consecuencia alcanzar un host de otra VLAN distinta a la del atacante.

Fuente: Ataques de Capa de Enlace de Datos (Bull, 2014)

Existen varias aplicaciones que los atacantes pueden utilizar como el yersinia, dsniff, macof, entre otras para realizar los ataques VLAN. Estas herramientas muestran a la gente cómo explotar redes mal configuración y debilidades físicas en la LAN.

2.2.2.6 *Ataques VLAN*

Las VLAN se implementan en la Capa de Enlace de Datos del modelo OSI. La mayoría de los ataques explotan la incapacidad de un switch para rastrear a un atacante, porque el switch no tiene un mecanismo inherente para detectar que se está produciendo un ataque. (Herón, 2013)

Esta debilidad significa que este mismo atacante puede realizar acciones maliciosas contra la ruta de red, alterando la ruta y explotando el cambio sin detección. (Herón, 2013). En la Tabla 7-2 se hace un breve resumen de las principales amenazas para las organizaciones que utilizan VLAN:

Tabla 7-2 Ataques VLAN	
Ataque	**Descripción**
CAM Table Overflow/ Media Access Control (MAC)	Este ataque se centra en la tabla CAM (Content Addressable Memory), que almacena información como direcciones MAC en un puerto físico junto con los parámetros de VLAN asociados. Las Tablas CAM tienen un tamaño fijo y eso es lo que las convierte en un objetivo para el ataque denominado **MAC Flooding o CAM Table Overflow**. Si la tabla CAM está llena, no se aceptan nuevas entradas y cuando la tabla CAM no puede almacenar más asociaciones MAC-Puerto el switch empieza a enviar por todos los puertos de que dispone (Broadcast) las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM, el switch empieza a comportarse como un hub.
Address Resolution Protocol (ARP)	Si un host transmite una solicitud ARP a la red, sólo espera que el host correspondiente responda. De manera similar, si un anfitrión anuncia su presencia enviando un ARP gratuito, otros anfitriones esperan que esté diciendo la verdad y crean lo que transmite, funciona bien hasta que aparezca un host malicioso. Cualquier elemento de un host legítimo se encaminará a través del host malicioso como puerta de enlace predeterminada. El atacante entonces empuja los datos a la puerta de enlace predeterminada real. Esto permitirá que el ataque vea el tráfico a la salida de la red, pero el tráfico entrante evitará al atacante. El atacante ahora necesita transmitir la dirección del host al que están intentando dirigirse en la LAN para obtener la puerta de enlace predeterminada para enviar los paquetes entrantes a sí mismo antes de transmitirlos a la víctima. Ahora puede ver todo el tráfico entrante y saliente.
Servidor de directivas de administración de VLAN (VMPS) / VLAN Query Protocol (VQP)	Este es un ataque poco probable ya que requiere que la red use VMPS. Es inusual ya que impone una carga significativa en los recursos administrativos de una empresa y Cisco, cuyo protocolo es 802.1X para la misma funcionalidad. Sin embargo, si se implementa, VMPS permite asignar VLAN en función de la dirección MAC del host y estas relaciones se almacenan en una base de datos. Esta base de datos suele ser descargada en el VMPS y luego consultada utilizando VQP, un protocolo no autenticado que utiliza UDP (User Datagram Protocol), lo que lo hace muy fácil de manipular por un atacante. Como resultado, mediante el uso de VQP, es muy fácil suplantar a los hosts ya que no hay autenticación, lo que permite al atacante unirse a una VLAN a la que no está autorizado a acceder. La mitigación consiste en monitorear la red por mal comportamiento, enviar consultas VQP fuera de banda o desactivar el

	protocolo
Ataque de fuerza bruta de multidifusión	Un ataque de fuerza bruta de multidifusión busca fallas en el software del conmutador. El atacante trata de explotar cualquier vulnerabilidad potencial en un switch, atacándolo con tramas multicast. Al igual que con el desbordamiento de CAM, el objetivo es ver si un conmutador que recibe una gran cantidad de tráfico multicast de capa 2 se "portará mal". El conmutador debe limitar el tráfico a su VLAN original, pero si el switch no maneja esto correctamente, las tramas pueden filtrarse en otras VLAN, si el enrutamiento las conecta.
Random Frame Stress	Este tipo de ataque casi podría considerarse "Fuzzying" pero en la Capa de Enlace de Datos. Se genera un gran número de paquetes, variando aleatoriamente varios campos dentro de cada paquete y dejando sólo las direcciones de origen y de destino sin tocar. El objetivo es ver cómo el software de conmutación hace frente a valores sin sentido o inesperados en los campos de paquetes. Este tipo de ataque debería fallar, pero obviamente se producen errores que pueden permitir un acceso inesperado a otras VLAN o dar lugar a ataques de negación de servicio (DoS).
Ataque de VLAN privada (PVLAN)	Las PVLAN se utilizan para dividir más grupos de hosts en la capa de Enlace de Datos. Por ejemplo, una zona desmilitarizada (DMZ) puede tener servidores web a los que accede el mundo exterior y un servidor sFTP (Secure File Transfer Protocol) que proporciona instalaciones de descarga para el personal en la campo. No hay ninguna razón para que estos servidores se comuniquen entre sí y las PVLAN evitarán que esto suceda. De hecho, PVLANs hacen que sea muy difícil para un servidor web infectado manchar un servidor sFTP, sin embargo, sólo lo hará en la capa
VLAN HOPPING	Los switches implementan VLANs, los usuarios se conectan a puertos de acceso que son miembros. VLAN HOPPING es cuando un usuario gana acceso a una VLAN no asignada al puerto del switch al cual el usuario se conecta.

Fuente: Ataques VLAN (Herón, 2013)

Elaborado por Pilamunga Norma, 2017

2.2.3 Ataques VLAN HOPPING

VLAN HOPPING es un método para atacar a los recursos en una VLAN. El concepto básico es tener acceso al tráfico en otras VLAN que normalmente no serían accesibles. Podemos decir entonces que un Ataque VLAN HOPPING es una vulnerabilidad de

seguridad en ambientes LAN que trabajan con puertos troncales, como se muestra en el Figura 7-2.

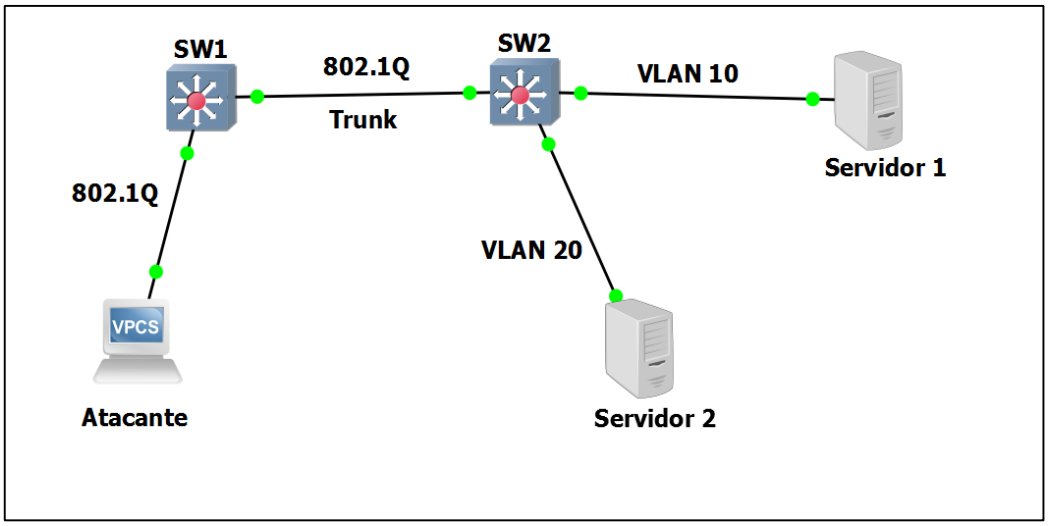


Figura 7-2 Ataque VLAN HOPPING

Fuente: Herrera, 2015

Elaborado por: Pilamunga Norma, 2017

En la Tabla 8-2 podemos observar una breve recopilación de las consecuencias que pueden provocar los ataques VLAN HOPPING que están diseñados para permitir que los atacantes pasen por alto un dispositivo de Capa 3 al comunicarse de una VLAN a otra no autorizada.

Tabla 8-2 Consecuencias Ataques VLAN HOPPING
1. El ataque funciona aprovechando un puerto de troncal configurado incorrectamente
2. El ataque no funciona en un solo switch porque la trama nunca será reenviada al destino pero en un entorno de múltiples switches, un enlace troncal podría explotarse para transmitir el paquete.
3. Se puede utilizar para robar contraseñas y otra información sensible de los usuarios de una red específica
4. También puede usarse para modificar, corromper o eliminar datos, instalar programas espía, propagar virus y troyanos en una red.
5. Puede desactivar cualquier medida de seguridad que los usuarios puedan tener en el dispositivo que mapea rutas entre las VLAN.

6.	Los hackers usan VLAN HOPPING para capturar información confidencial, como detalles de cuentas bancarias y contraseñas de suscriptores de redes.

Fuente: Consecuencias Ataques VLAN HOPPING (Baxevanos, 2014; Herón, 2013)
Elaborado por Pilamunga Norma, 2017

Para aprovechar los huecos de seguridad en una red LAN, a través de VLAN HOPPING podemos hacer uso de 2 métodos de ataque:

- Switch Spoofing
- Double Tagging

2.2.3.1 *Ataque Switch Spoofing*

Uno de los ataques comunes en VLANs suele ser el ataque de Switch Spoofing (Suplantación de Switch), es decir el atacante de red configura un equipo para simular que es un switch emulando ISL o 802.1Q y señalización DTP, (Deivid, 2016).

Este ataque se basa en protocolo de troncal dinámico (DTP). DTP se utiliza para negociación de un enlace entre dos dispositivos y para negociar el tipo de encapsulación trunking (802.1Q) que se utilizará.(Rouiller, 2006)

Este ataque hace que el atacante de red se conecte a un switch Cisco no autorizado y parezca ser un switch con un puerto troncal y cuando establece el enlace será capaz de ver todas las VLANs. (Baxevanos, 2014)

2.2.3.1.1 *Fases Ataque Switch Spoofing*

1. En el Figura 8-2, el atacante conecta un cable en un puerto del switch no autorizado, mismo que está configurado de manera predeterminada como Dynamic Desirable.

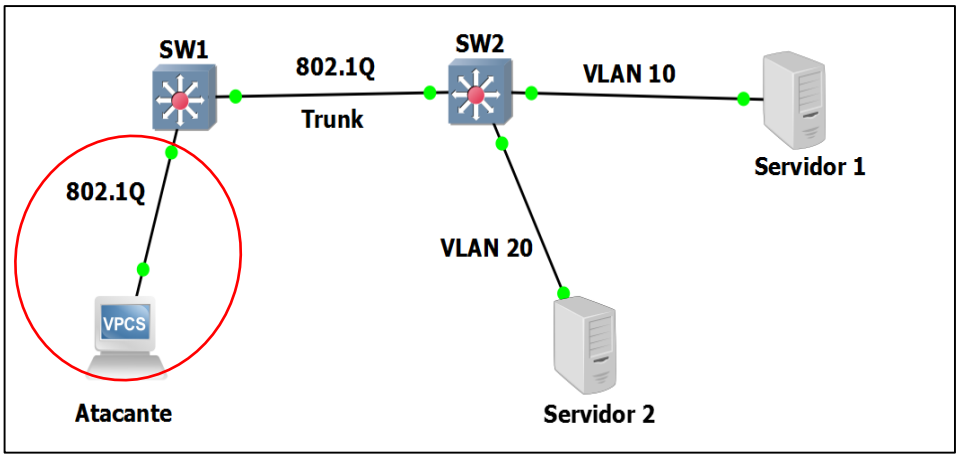


Figura 8-2 Atacante conecta cable en un puerto del switch no autorizado

Fuente: Herrera, 2015

Elaborado por: Pilamunga Norma, 2017

2. Al simular un enlace trunk ISL o 802.1Q, el atacante está en modo trunking o en el modo de negociación automática DTP, como se observa en el Figura 9-2.

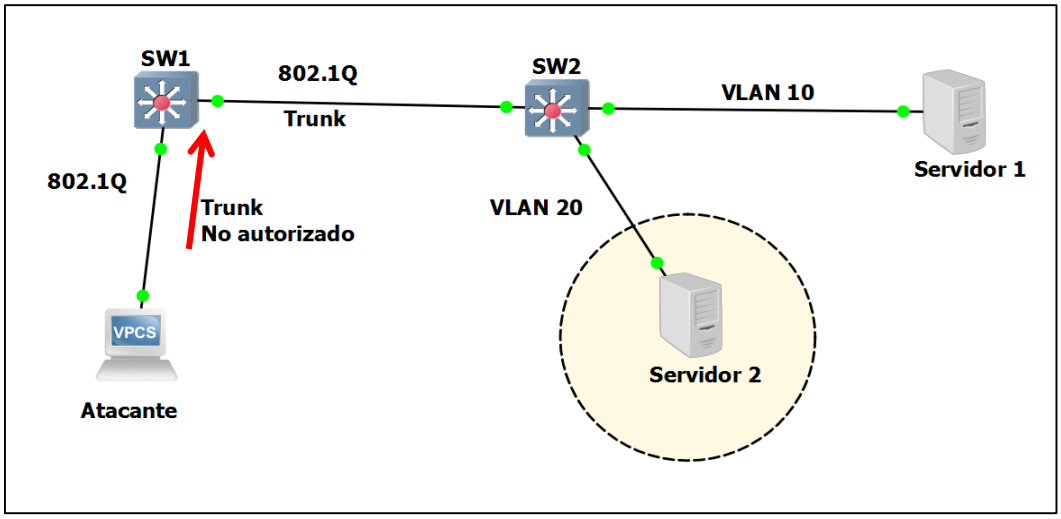


Figura 9-2 Atacante conecta cable en un puerto del switch no autorizado

Fuente: Herrera, 2015

Elaborado por: Pilamunga Norma, 2017

Aprovechando la capacidad dentro del switch se determina automáticamente lo que está conectada al puerto individual Figura 10-2, si se trata de un puerto de acceso, sería un dispositivo de usuario final y si lo que se está conectado es una interfaz troncal, se configura automáticamente. Y se produce el ataque. (Baxevanos, 2014)

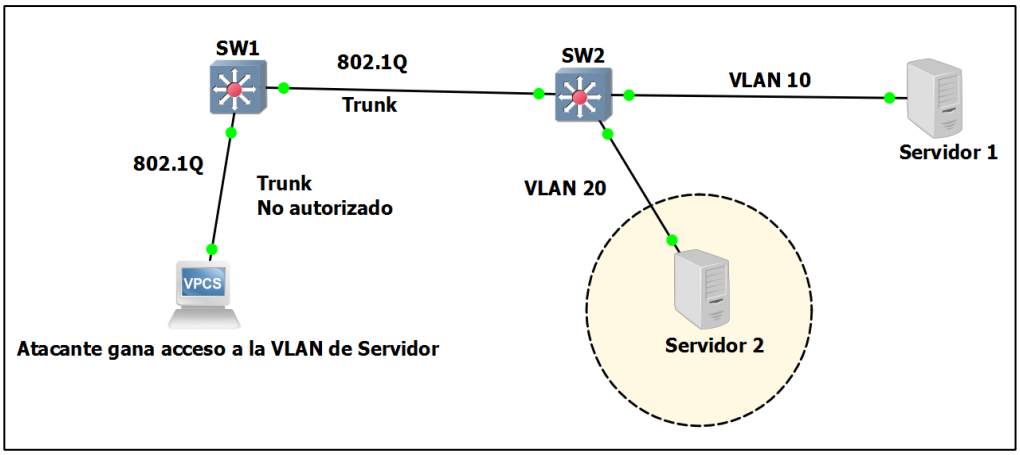


Figura 10-2 Enlace Trunk establecido

Fuente: Baxevanos, 2014

Elaborado por: Pilamunga Norma, 2017

2.2.3.1.2 *Consecuencias Ataque Switch Spoofing*

El ataque Switch Spoofing es explotado cuando las interfaces están configuración para negociar un trunk y si tiene éxito entonces:

- "El sistema del atacante adquiere un enlace trunk al switch
- El atacante puede enviar paquetes para cualquier VLAN soportada por el enlace trunk
- El atacante puede comunicarse con cualquier dispositivo en cualquiera de las VLAN asociadas
- La comunicación bidireccional puede ocurrir entre el atacante y un nodo objetivo porque el atacante puede colocarse en la red VLAN
- También permite al atacante escuchar el tráfico dentro de una VLAN de destino" (Bull, 2015)

2.2.3.2 *Ataque Double Tagging.*

En un ataque Double Tagging, el atacante 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. Este ataque aprovecha que la mayoría de switches sólo realiza un nivel de desencapsulación. (Muñoz, 2011)

El ataque Double Tagging puede ocurrir cuando la VLAN de un puerto de acceso es igual a la VLAN de un enlace troncal, de esta forma el atacante puede realizar el ataque, ya que etiqueta la trama con la ID de VLAN a la que desea llegar y luego lo etiqueta con la ID de su VLAN. (Deivid, 2016)

Este tipo de ataque funciona aun cuando los puertos troncales están desactivados. (Baxevanos, 2014). Podemos observar en el Figura 11-2 las Etapas de un Ataque Double Tagging.

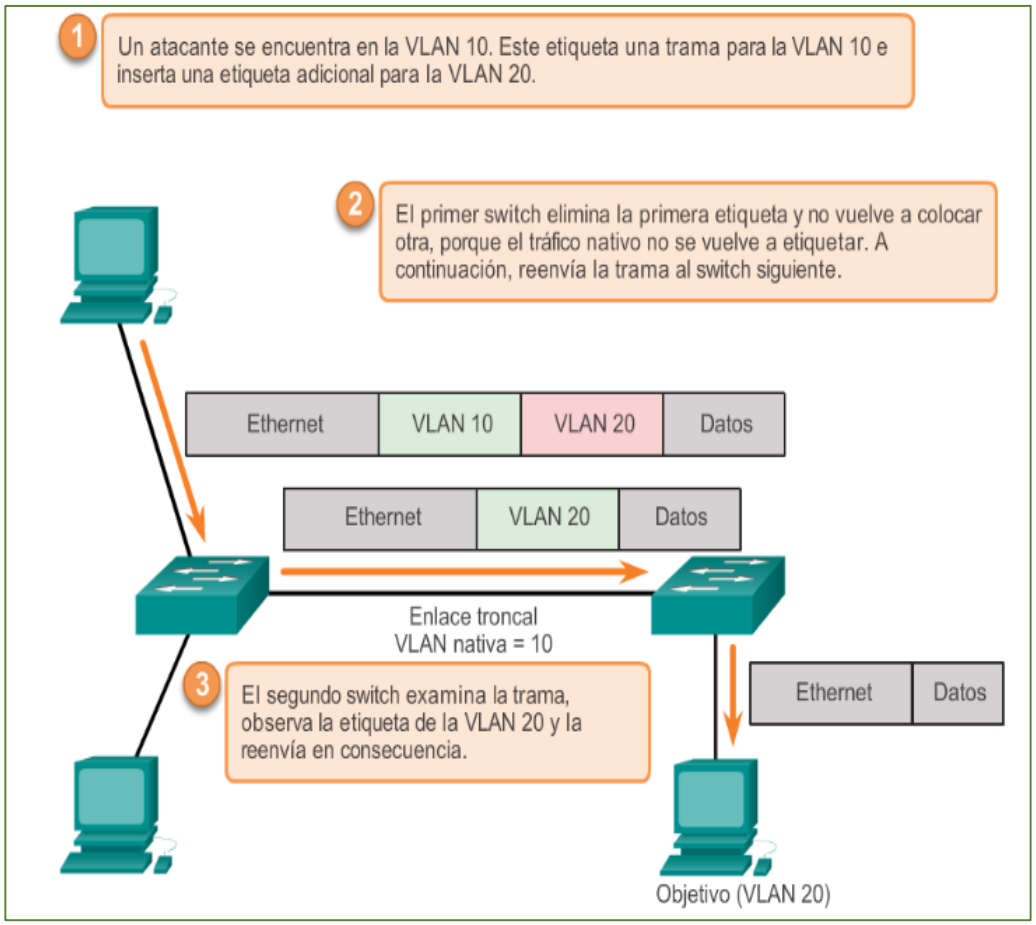


Figura 11-2 Etapas Ataque Double Tagging

Fuente: Deivid, 2016

2.2.3.2.1 *Consecuencias Ataque Double Tagging.*

Al tener éxito con el ataque Double Tagging, podemos generar nuevos ataques por el mismo hecho que somos parte de la VLAN; es decir podemos realizar un ARP Poisong, ARP Spoofing, un ataque Dos entre otros, es decir tenemos consecuencias como:

- “El atacante puede enviar paquetes a una VLAN de destino
- El sistema objetivo no puede responder de nuevo
  - El sistema de ataque está en la VLAN nativa
  - El objetivo se encuentra en una VLAN de acceso aislada del dominio de broadcast de la VLAN nativa
- No es un buen ataque para escuchar la red
- Excelente método para ataques DoS” (Bull, 2015)

2.2.4 Vulnerabilidades de seguridad para Ataques VLAN HOPPING

Las fallas de seguridad en la configuración de las infraestructuras de red implementadas con VLAN, dan lugar a accesos no autorizados. La Tabla 9-2 muestra las vulnerabilidades más comunes de los Ataque VLAN HOPPING.

Tabla 9-2 Vulnerabilidades Ataques VLAN HOPPING	
1.	DTP habilitado en los switch Cisco por defecto
2.	Configuración automática de los trunk 802.1Q
3.	Pobre configuración de los puertos. (puertos troncales no configurados)
4.	Puertos troncales presentes en la misma VLAN nativa que el atacante
5.	Un solo nivel de desencapsulación
6.	Uso de la VLAN NATIVA (VLAN 1)
7.	Puertos sin uso habilitados
8.	Ausencia de políticas de seguridad
9.	Nivel de conocimiento alto del atacante interno
10.	Usuarios con prioridades dentro de la organización
11.	Accesos no autorizados
12.	Falta de monitorización de la red

Fuente: Vulnerabilidades Ataques VLAN HOPPING

Elaborado por Pilamunga Norma, 2017

Debido a que el usuario interno es la principal amenaza para vulnerar la infraestructura de red por los privilegios y permisos que tienen dentro de la organización, se lista las amenazas que están asociadas con la seguridad de la red de datos mismas que se identifican mediante la observación y en base a ISO/IEC 27002 donde se analiza la seguridad física y la información de las configuraciones de los equipos.

La Tabla 10-2 muestra las amenazas que pueden ser el punto de partida para para identificar otras amenazas o infracciones potenciales dentro de la red interna y comprometer la confidencialidad, autentificación e integridad, una vez que haya éxito del Ataque VLAN HOPPING.

Tabla 10-2 Amenazas Confidencialidad, Autentificación e Integridad frente a VLAN HOPPING	
Confidencialidad	
Amenazas	**Consecuencias**
Escuchar información en la red	Se pierde la privacidad
Facilita el análisis del tráfico	Se puede identificar patrones de acceso
Descubre la configuración de la red	Abre la puerta para otros ataques
Autentificación	
Suplantación de Identidad. El atacante simula ser un switch	Máquina penetrada. Facilita otros ataques
Integridad	
Tramas modificadas Doble Tagging	Facilita ataque DoS

Fuente: Amenazas Confidencialidad, Autentificación e Integridad frente a VLAN HOPPING

Elaborado por Pilamunga Norma, 2017

Se habla de consecuencias frente a un Ataque VLAN HOPPING cuando hay factores de riesgos que ayudan a provocar alteraciones a la infraestructura de red como se resume en la Tabla 11-2

Tabla 11-2 Consecuencias y medidas frente a un Ataque VLAN HOPPING			
Activo	**Factor de riesgo**	**Consecuencia**	**Como proteger**
Cableado, Switches, Router	Conexiones de cableado no protegidas	Daños en el cableado Robo de datos mediante Switch Spoofing y Double Tagging	Políticas de seguridad
	Longitud de los cables de red excedida sin protección	Cable de red expuesto	Políticas de seguridad Mantenimiento del cableado.
	Pobre configuración de los equipos de red	Accesos a información por parte de personal interno sin autorización	Manuales de configuración de la red
	Puertos abiertos del switch	Posibles intrusiones y robo o divulgación de información.	Política de seguridad - Configuración de puertos y herramientas de monitoreo de puertos.

	Switch spoofing y Double Tagging	Acceso a la infraestructura de red	Políticas de seguridad Controles de seguridad física
Administrador de red	Deficiencias de contraseñas	Uso indebido de derechos de administrador	Políticas de seguridad
	Deficiencias conceptuales en la red	Mala configuración de la red	Políticas de seguridad
	Mal uso de derechos de administrador	Mala distribución de los permisos y de las cuentas de administrador.	Políticas de seguridad Levantamiento de documentación
	Reglas insuficientes o ausencia de ellas	Mal manejo de los Centros Tecnológicos	Políticas de seguridad Levantamiento de documentación
	Configuración inadecuada de componentes de red	Errores de transmisión, interrupción del servicio de red.	Políticas de seguridad Equipamiento de red
	Deficiencias conceptuales en la red	Mal manejo de la red	Políticas de seguridad Capacitación al personal
	Falta de autenticación	Posibles intrusiones y robo o divulgación de información.	Políticas de seguridad - Controles de acceso a datos y a equipos, y firewall.
Usuarios	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de la información	Políticas de seguridad - Capacitación
	Entrada sin autorización a departamentos	Robo de equipos o insumos, divulgación de datos.	Política de Seguridad Control de acceso físico
	Entrenamiento de usuarios inadecuado	Predisposición a errores y bajo rendimiento de usuarios.	Política de Seguridad - Capacitación
	Incumplimiento de las medidas de seguridad del sistema	Medidas correctivas tomadas por la gerencia, según la gravedad del incidente.	Política de Seguridad
	Desvinculación del personal	Robo o modificación de información, sabotaje interno.	Políticas, normas internas
	Uso de derechos sin autorización	Mal manejo de la información	Políticas y normas internas
	Manejo inadecuado de responsabilidades y roles del personal de sistemas	Inadecuada asignación de responsabilidades	Políticas de seguridad

Fuente: Consecuencias y medidas frente a un Ataque VLAN HOPPING

Elaborado por Pilamunga Norma, 2017

2.2.5 Políticas de Seguridad

Una política de seguridad es el conjunto de procedimientos, normas, reglas para proteger redes y sistemas dentro de una organización con el fin de prevenir, detectar o corregir accesos no autorizados.

Las organizaciones van de la mano con la tecnología; y su infraestructura de red es un tema importante que no se debe subestimar dado que las fallas de seguridad provienen del interior de la red, es aquí donde la mitigación de ataques es parte de la seguridad y

esta se relaciona con la protección de los recursos y la información a través de la implementación de políticas de seguridad.

Para crear una política de seguridad nos basaremos en las normas ISO que son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). (Collazos, 2013).

2.2.6 Normas ISO 27000

La norma ISO 27000 es una norma internacional y abierta, cuyo objetivo es establecer los requisitos mínimos con los que debe cumplir un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización. Para nuestro estudio haremos uso de la norma 27002: 2013

2.2.6.1 *Normas ISO 27002*

Las normas ISO/IEC 27001, ISO/IEC 27002 están enfocadas a todo tipo de organizaciones (por ej. empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza.(López & Ruiz, 2012)

La Norma ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. (López & Ruiz, 2012).

Uno de los objetivos es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.(López & Ruiz, 2012). La ISO/IEC 27002:2013 está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles. (Ver Anexo 2)

Ahora el definir una política de seguridad significa incluir el marco general y los objetivos de seguridad de la información de la organización, teniendo en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad y es ahí donde los controles de la ISO/IEC 27002:2013 tiene gran relevancia.

Para esta investigación haremos uso de las recomendaciones que son el resultado de los controles de los dominios de la Norma 27002, con la que levantaremos el documento de las políticas de seguridad como un recurso para mitigar las vulnerabilidades de los ataques VLAN HOPPING, tomando en consideración 7 de los 14 objetivos:

1. **Políticas de Seguridad de la Información:** Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior. (Ges, 2013)
2. **Seguridad relativa a los recursos humanos**: "Si analizamos los incidentes de seguridad que se producen en una organización nos daremos cuenta de que la gran mayoría de estos tienen su origen en un error humano. Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir." (Ges, 2013)

3. **Control de acceso**: Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo no todas las personas de una organización necesitan acceder para realizar su actividad diarias a todos los datos, sino que tendremos roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, etc. siendo algunos de los controles que se incluyen en este apartado. (Ges, 2013)
    - "Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.
    - Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

- Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema." (López & Ruiz, 2012)

4. **Seguridad física y del entorno:** La seguridad no es solo a nivel tecnológico sino también físico, es decir, no dejar accesos libres a los lugares donde están los servidores, por parte del personal externo los documentos con los que se están trabajando no sólo nos permitirán gestionar de forma adecuada la seguridad sino que se acabarán convirtiendo en hábitos que nos aportan eficiencia en la gestión

5. **Seguridad de las comunicaciones:** Partiendo de la base de que la gran mayoría de los intercambios de información y de datos en distintas escalas se llevan a cabo mediante las redes sociales, garantizar la seguridad y proteger de forma adecuada los medios de transmisión de estos datos clave. (Ges, 2013)

    - "Asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.
    - La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.
    - La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección.
    - Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante." (López & Ruiz, 2012)

6. **Gestión de incidentes de seguridad de la información: "**No podemos hablar de controles de seguridad sin mencionar un elemento clave, los incidentes en seguridad, hay que estar preparado para cuando estos incidentes ocurran, dando una respuesta rápida y eficiente siendo la clave para prevenirlos en el futuro. Se deberían controlar los accesos a servicios internos conectados en red." (Ges, 2013)
    - "El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

a. que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones;
b. que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos;
c. el cumplimiento del control de los accesos de los usuarios a los servicios de información.

- Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones
- Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades. ” (López & Ruiz, 2012)

7. **Cumplimiento:** “No podemos hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que se encuentre relacionadas con este campo y con las que conviven en las organizaciones. Debemos tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben garantizar que se cumple y que están actualizados con los últimos cambios siendo esencial para no llevarnos sorpresas desagradables.”(Ges, 2013)

Con este antecedente, nuestro reto es que las organizaciones hagan frente a la ciberdelincuencia, para lo cual se requiere de una buena gestión y de procedimientos adecuados, es ahí donde se hace uso de la Norma ISO para esta investigación la 27002 que sirve de guía para ayudar a implantar los sistemas de gestión de seguridad de la información, aquí es donde se definen políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles una vez establecidos e implementados deben revisarse y mejorarse de forma constante para asegurarse que son efectivos ya que es un importante motor de desarrollo de la sociedad digital y por tanto de la economía.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

En este apartado se define el tipo de investigación a utilizarse, diseño, métodos, técnicas e instrumentos con su respectiva validación, con el objetivo de implementar políticas de seguridad para mitigar las vulnerabilidades de los ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN.

3.1 Diseño de la Investigación

Esta investigación es de tipo CUASI-EXPERIMENTAL, porque se experimenta con uso de escenario de pruebas para los ataques VLAN HOPPING. Se refiere a diseños de investigación experimentales en los cuales los ataques de estudio no están asignados aleatoriamente.

3.2 Tipo de Estudio

El tipo de estudio es científico; de tipo aplicada, porque se basa en los conocimientos existentes; de nivel exploratorio y descriptivo, porque permite detallar y explicar las vulnerabilidades como resultado de la falta de políticas de seguridad para contrarrestar a los ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN.

3.3 Métodos, técnicas e instrumentos

En este apartado se describe los métodos, técnicas e instrumentos requeridos para la investigación.

3.3.1 Métodos de Investigación

El método seleccionado es el científico, de tipo mixta porque contienen aspectos cualitativos y cuantitativos, también es exploratoria, descriptiva y documental,

mediante el cual se realiza la observación sistemática que dan lugar a la formulación del problema: las vulnerabilidades de los ataques VLAN HOPPING, formular la hipótesis basada en el razonamiento deductivo y mediante la experimentación se levanta los escenarios de prueba adecuados para finalmente analizar los resultados obtenidos de modo que permitan obtener soluciones apropiadas para cumplir con la hipótesis de la investigación es decir confirmar o rechazar la hipótesis propuesta.

3.4 Población de estudio

Para el cálculo de la muestra de la investigación se tomó los datos del INEC; donde en la ciudad de Riobamba existen 92 empresas entre grandes, medianas y pequeñas son socios de la Cámara de Industrias de Chimborazo.

3.5 Selección de la muestra

Para la selección de la muestra se hace uso de los criterios de inclusión y exclusión y se selecciona 30 organizaciones que cumplen con el requerimiento como es tener implementado VLAN.

3.5.1 Criterios de Inclusión de la muestra

- Organizaciones con infraestructura de red implementadas con tecnologías de seguridad VLAN

3.5.2 Criterios de Exclusión

- No cuenta con infraestructura de red básica no cumple requerimiento para ejecutar el ataque.

3.6 Tamaño de la muestra

Del total de 30 organizaciones se aplicó el cálculo de la muestra dando como resultado 12 organizaciones, donde se realizó la encuesta dirigida a los administradores de red.

Tamaño de la Población (N)	30
Error Muestral (E)	0,07
Proporción de Éxito (P)	0,9
Proporción de Fracaso (Q)	0,1
Valor para Confianza (Z) (1)	1,96

(1) Si: Z

Confianza el 99%	2,32
Confianza el 97.5%	1,96
Confianza el 95%	1,65
Confianza el 90%	1,28

Fórmula para muestra para poblaciones finitas

Variable	Atributo
$n = \frac{s^2 * z^2}{E^2}$	$n = \frac{z^2 * P * Q}{E^2}$

Dónde:

S^2 = Varianza
Z = Valor normal
E = Error
N = Población
P = Proporción
Q = 1-P

Tamaño de Muestra

Fórmula	21
Muestra Óptima	**12**

3.6.1 Técnicas de recolección de datos

Para esta investigación se hace uso de las siguientes técnicas:

- **Búsqueda de información:** a través de esta técnica se obtiene fuentes de información avalada por expertos en el tema y validada por la comunidad científica.

- **Pruebas:** a través de pruebas de concepto se demuestra que una aplicación o servicio puede ser vulnerable, es decir se realiza experimentos en escenarios de laboratorio.

- **Observación:** esta técnica permite obtener información registrada durante el experimento que se obtiene a través de las pruebas de concepto en los escenarios de laboratorio.

3.7 Instrumentos de recolección de datos

En la tabla 1-3 se resume los instrumentos requeridos en la presente investigación para recopilar la información:

Tabla 1-3 Instrumentos

Instrumentos	**Descripción**
GNS3 1.5.3	Es un simulador Gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos(De Nova, 2012). Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: ▪ Dynamips, emulador de IOS que ejecutar imágenes binarias de los IOS de Cisco Systems. ▪ Dynagen, un front-end basado en texto para Dynamips (De Nova, 2012) ▪ Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco o las personas que quieren pasar sus CCNA, CCNP, CCIE DAC o certificaciones.
VMware Inc	Software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player.
Yersinia	Herramienta utilizada para probar la seguridad de la capa 2. Yersinia es una herramienta de red diseñada para tomar ventaja de algunas debilidades en los diferentes protocolos de red. Permite analizar y probar redes y sistemas. En resumen Yersinia permite descubrir determinadas vulnerabilidades de la Capa de Enlace de Datos. Permite analizar y comprobar redes y sistemas. Soporta los protocolos: ✓ Spanning Tree Protocol (STP) ✓ Cisco Discovery Protocol (CDP) ✓ Dynamic Trunking Protocol (DTP) ✓ Dynamic Host Configuration Protocol (DHCP) ✓ Hot Standby Router Protocol (HSRP)

	✓ IEEE 802.1q, Inter-Switch Link Protocol (ISL) ✓ VLAN Trunking Protocol (VTP)
Cisco IOS	Es el software (piense en "sistema operativo") que se utiliza en muchos de los routers y conmutadores de Cisco, especialmente los que va a trabajar con el progreso hacia el CCNA. Cisco simplemente compila el mismo código IOS para ejecutar en sistemas operativos Unix (Solaris, Linux, OS X, y tal vez otros) para ser utilizados por ingenieros de Cisco y algunos clientes afortunados.
Wireshark	Se trata de un analizador de protocolos, que nos permite analizar todo el tráfico de una red ethernet, aunque también se puede utilizar en redes de otro tipo, estableciendo la configuración en modo promiscuo lo que le permite capturar todo el tráfico de la LAN.
Centos 6	Es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito.
Kali Linux	Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

Fuente: Instrumentos

Elaborado por Pilamunga Norma, 2017

3.8 Metodología para mitigar las vulnerabilidades de los ataques VLAN HOPPING

Para realizar una valoración integral de las debilidades a nivel de la LAN se sigue la metodología del Pentesting que permite medir el nivel de seguridad en una red.

Un Pentesting es un test de Intrusión o penetración donde se evalúan minuciosamente y cuidadosamente los niveles de seguridad en redes, sistemas de computación y aplicaciones involucradas en los mismos. Con el test de intrusión se analiza la efectividad de los controles de seguridad implantados realizándose acciones planificadas que simulan el comportamiento de un atacante. (Díaz, 2014). El objetivo del test de Pentesting es vulnerar la seguridad del sistema de información de la organización para conseguir accesos no autorizados, interrumpir un servicio u obtener información sensible entre otros. (Díaz, 2014)

Podemos diferenciar tres tipos de test de penetración o intrusión:

1. **Caja Negra** (Black box): "En este tipo de test de intrusión, el atacante no posee ninguna información previa sobre el cliente, excepto lo que este publica voluntariamente en sus sistemas de información. El atacante deberá actuar de la misma forma que lo haría un atacante externo que intenta explotar vulnerabilidades del sistema o extraer información privada contenida en este." (Díaz, 2014)

2. **Caja Blanca (**White box): "Se posee un amplio conocimiento de la organización, principalmente su estructura, y de la red. Simula un atacante con un conocimiento exhaustivo del sistema tomando de este modo el punto de vista, por ejemplo, de un administrador o usuario que cuentan con acceso al sistema de información de la organización". (Díaz, 2014)

3. **Caja Gris (Grey box):** "Es una combinación de los dos métodos anteriores, simula que es un atacante real ejecuta ataques similares a los de caja negra. Este test dispone de información técnica sobre el sistema lo que permite identificar un mayor número de amenazas". (Díaz, 2014)

Como referencia las metodologías de seguridad existentes son: OSSTMM (Open Source Security Testing Methodology Manual) y NIST 800-115 (National Institute of Standards and Technology). OSSTMM permite identificar claramente el alcance de cada una de las siguientes actividades" (Herzog, 2003):

- **Búsqueda de Vulnerabilidades:** específicamente nos basaremos en el punto Búsqueda y Verificación de Vulnerabilidades:

  - ✓ "La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red." (Herzog, 2003)

  - ✓ "La investigación concerniente a la búsqueda de vulnerabilidades es necesaria hasta prácticamente el momento de la entrega del informe." (Herzog, 2003)

  - ✓ "La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. No obstante, es necesaria la verificación manual para eliminar falsos positivos, expandir el ámbito de hacking y descubrir el flujo de datos de entrada y salida de la red. La búsqueda manual de vulnerabilidades hace referencia a las personas que delante del ordenador utilizan la creatividad, la experiencia y la ingenuidad para probar la red objetivo." (Herzog, 2003)

- **Escaneo de la Seguridad**: Orientado a búsquedas de vulnerabilidades en el sistema, identificación de puntos débiles los sistemas y análisis individualizado. (Herzog, 2003)

- **Test de Intrusión:** Se plantean test de pruebas que se centran en romper la seguridad de un sistema determinado. (Herzog, 2003)

- **Evaluación de Riesgo:** Se refiere a los análisis de seguridad, a través de entrevistas e investigación de nivel. (Herzog, 2003)

- **Auditoría de Seguridad:** Continua inspección a los sistemas, por parte de los administradores que controlan, el cumplimiento de las políticas de seguridad definidas. (Herzog, 2003)

- **Hacking Ético**: Obtener objetivos complejos, dentro de la red de sistemas, a partir de los test de intrusión. (Herzog, 2003)

Para el desarrollo de la presente investigación seguimos las cuatro fases del pentesting como se muestra en la Figura 1-3:

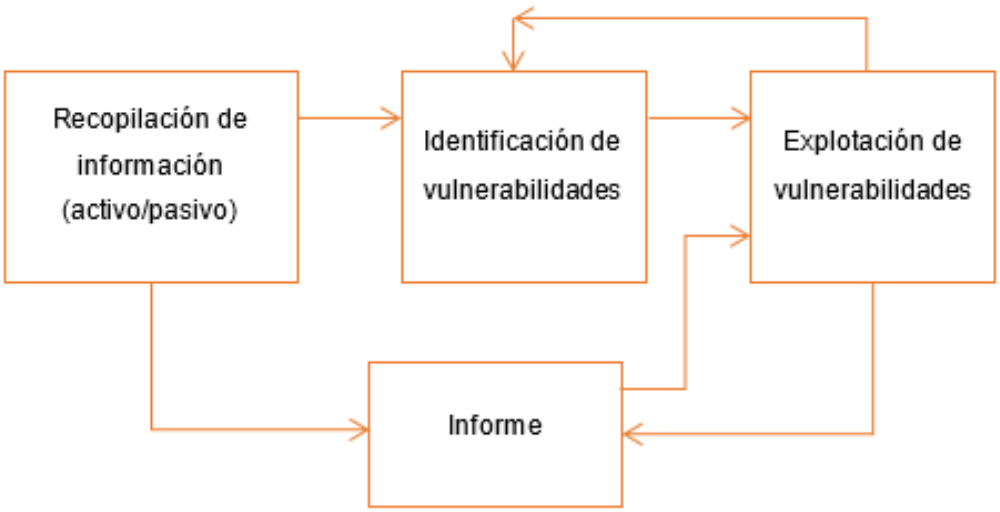


Figura 1-3 Metodología

Fuente: Monroy, 2011

3.8.1 Fase 1. Recopilación de información:

Consiste en obtener información del sistema/organización/red/máquina bajo un análisis y con el uso de diferentes herramientas que cumplen este propósito.

Tienen en esta fase especial interés las técnicas y ataques de ingeniería social (Díaz, 2014). En esta fase no se busca ninguna vulnerabilidad sino se prepara y planifica para obtener la mayor cantidad de información referente a los equipos de la red objetivo.

Dentro de esta fase se aplicó encuestas dirigidas a los administradores de red, para identificar la problemática existente.

3.8.1.1 *Escenario de pruebas*

En esta fase se levanta el escenario de prueba, con la topología más común utilizada en las 12 organizaciones encuestadas con el propósito de mitigar las vulnerabilidades de los ataques VLAN HOPPING en la Capa de Enlace de Datos y elaborar las políticas como se muestra en la Figura 2-3.

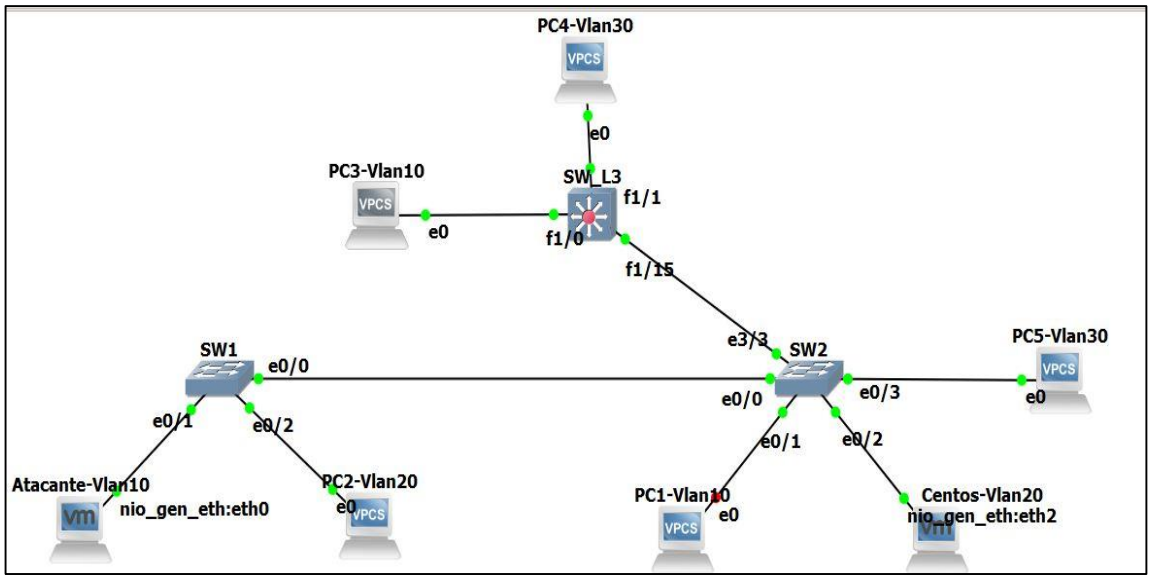


Gráfico 1-3 Escenario de pruebas

Elaborado por: Pilamunga Norma, 2017

El mapeo de la red incluye la topología y se identifica los dispositivos empleados en la topología de red simulada, las características de los equipos y dispositivos se describen en la Tabla 2-3.

Tabla 2-3 Listado de dispositivos de red Simulada

Dispositivos de red	Detalle
Máquina virtual (Virtualbox)	VMware® Workstation 12 Pro. Intel. Core (TM) i7-6500U CPU @2.50Ghz 2.60Ghz
Switch Capa 2	Marca Cisco IOU generic. Modelo Imagen i86bi-linux-l2-adventereprisek9-15.2d.bin IOS CISCO, administrable. Número de puertos:16 puertos
Switch Capa 3	Marca Cisco. Modelo 3745 256MB RAM. Image C3745 256MB RAM. Image c4735-advipservicesK9-mz.124-25d.image
Pc victima	Máquina Centos 6.
VPCS	Virtual PC Simulator 2 MB de RAM
Pc Atacante	Máquina con Kali Linux

Fuente: Listado de dispositivos de red Simulada

Elaborado por: Pilamunga Norma, 2017

3.8.1.2 *Configuraciones*

Tienen sistemas operativos IOU (**Cisco IOS on UNIX (IOU).** Es una versión totalmente funcional de IOS que se ejecuta como un modo de usuario UNIX (Solaris). IOU se construye como una imagen nativa de Solaris y se ejecuta como cualquier otro programa. IOU apoya todos los protocolos y características independientes de la plataforma.) Los Switches de capa 2 funcionan sobre la máquina Virtual de GNS3 en Linux. Las configuraciones se detallan en el Anexo 3, donde se encuentra paso a paso el levantamiento de:

1. Switch 1 y 2,
2. Router, donde únicamente se configuró Inter VLAN Routing, pero para esta prueba no se utilizará ya que como se verá más adelante los PCs no tienen puerta de enlace por lo que solo pueden comunicarse con otros equipos en la misma VLAN,
3. Se configura direcciones IP para las VPCs.
4. Centos PC

3.8.1.3 *Pruebas de conexión entre Pcs*

1. Una vez establecidos las direcciones IP, se verifica que la dirección IP perteneciente a la VLAN 10 no cuenta con una puerta de enlace para poder comunicarse con otras VLAN. Gráfico 2-3.

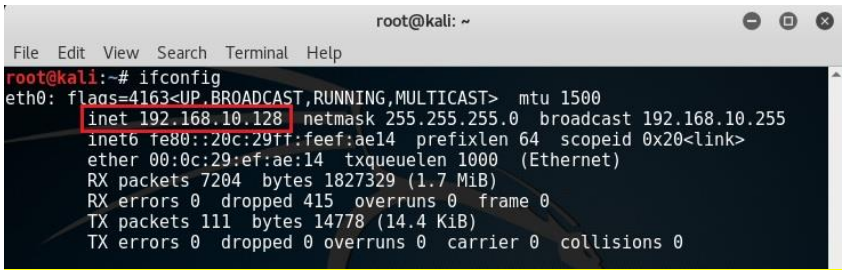


Gráfico 2-3 IP VLAN 10

Elaborado por: Pilamunga Norma, 2017

2. Se comprueba que no hay ruteo como se muestra en el Gráfico 3-3.

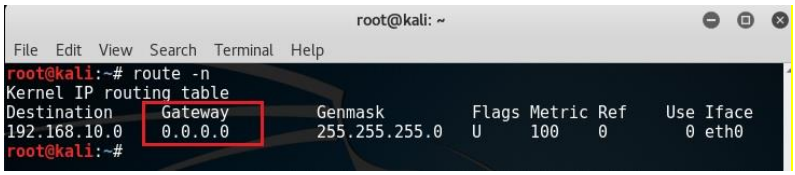


Gráfico 3-3 Ruteo

Elaborado por: Pilamunga Norma, 2017

3. Pruebas de conexión entre las dos máquinas que están en la misma VLAN 10 conectadas en diferentes switches. Gráfico 4-3

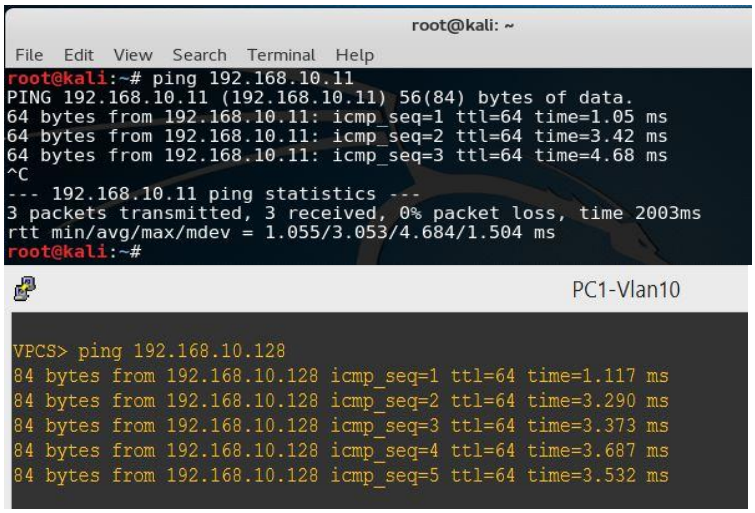


Gráfico 4-3 Ping entre atacante y PC1-Vlan10

Elaborado por: **Pilamunga Norma, 2017**

4. Se comprueba que no hay conexión entre la VLAN 10 y 20. Gráfico 5-3

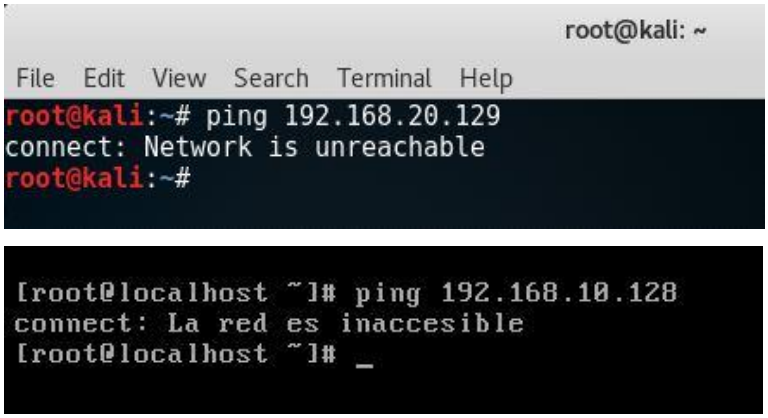


Gráfico 5-3 Ping entre Atacante y Centos-Vlan20 y viceversa.

Elaborado por: Pilamunga Norma, 2017

3.8.2 Fase 2. Identificación de vulnerabilidades

En esta etapa se realizan pruebas y test para identificar recursos específicos y características concretas. Se intenta localizar las posibles y potenciales vulnerabilidades se hace uso de la herramienta Wireshark. (Díaz, 2014).

Los switches son los dispositivos más importantes en la Capa de Enlace de Datos y por tanto la seguridad del enlace depende de su correcta configuración, cuando no sucede así dejamos abiertos huecos de seguridad donde el atacante aprovecha las vulnerabilidades para tener acceso no autorizado a la red y siendo el usuario interno la principal amenaza para vulnerar la infraestructura de red por los privilegios y permisos que tienen dentro de la organización, se deben establecer medidas y normas que ayuden a protegernos de los ataques VLAN HOPPING.

1. Una vez que se tiene identificado la infraestructura de red con segmentación mediante VLAN, comienza el proceso de descubrimiento de la VLAN y su identificador a través del sniffing pasivo, desde la máquina atacante, máquina virtual de Kali Linux que está siendo ejecutada en VMWare e integrada a GNS3, como se muestra el Gráfico 6-3.

Gráfico 6-3 Pc Atacante

Elaborado por Pilamunga Norma, 2017

2. Hacemos uso de Wireshark para obtener información a través de la captura de tráfico, Gráfico 7-3 y Gráfico 8-3.

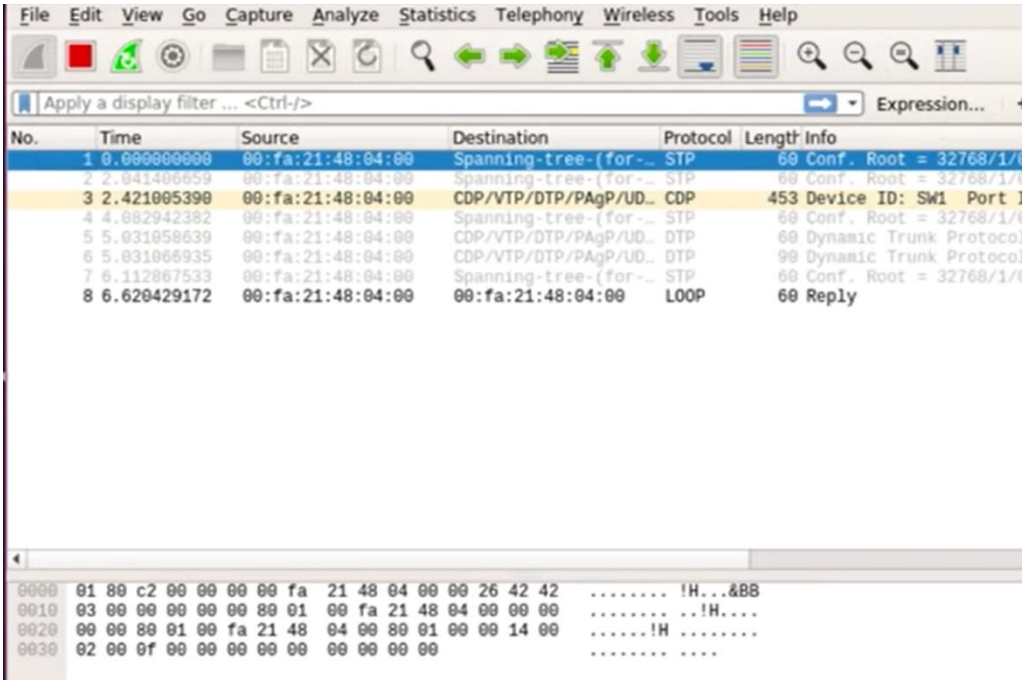


Gráfico 7-3 Captura de tráfico usando Wireshark

Elaborado por: Pilamunga Norma, 2017

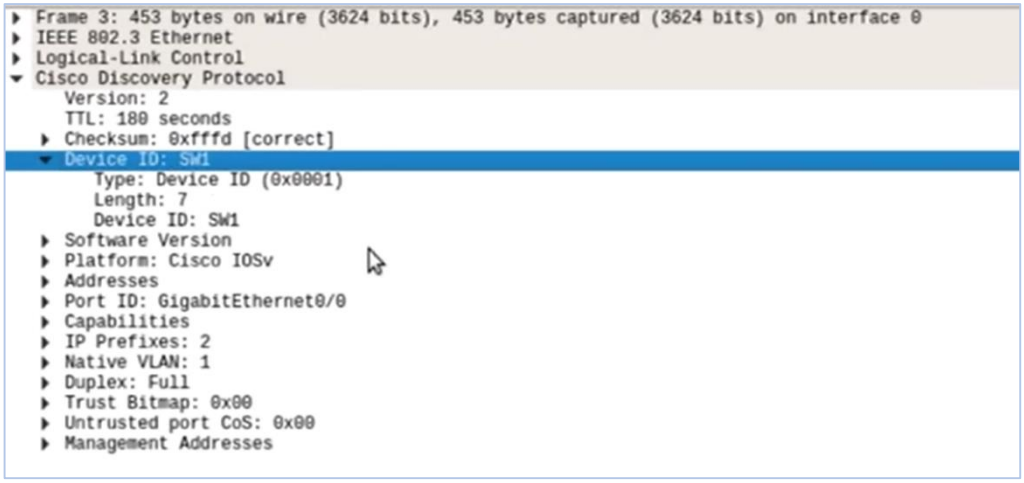


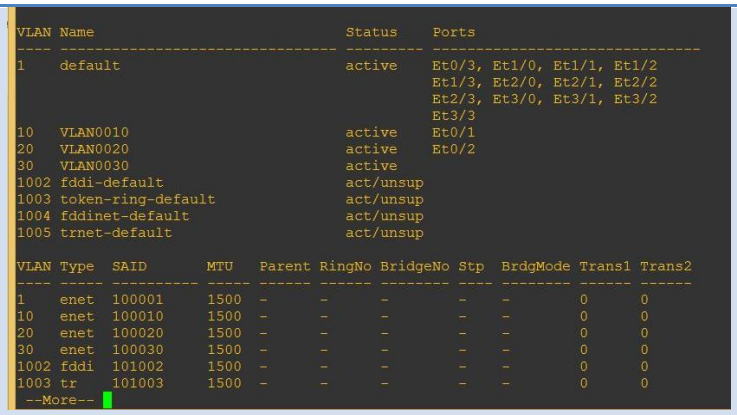
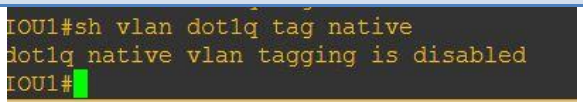
Gráfico 8-3 Captura de tráfico

Elaborado por: Pilamunga Norma, 2017

3. Luego del sniffing pasivo se lista las vulnerabilidades Tabla 3-3 producto de sistemas incorrectamente configurados por la inexperiencia, falta de entrenamiento, quenimportismo por parte del personal técnico así como las fallas de administración esto es la falta de monitorización de la red, documentación, ausencia de políticas de seguridad entre otras.

Tabla 3-3 Vulnerabilidades encontradas en el Escenario de Pruebas planteado

▪ DTP Activado ▪ Trunk negociación ▪ VLAN nativa 1 ▪ Puertos en no mode "Access"	SW1 Name: Et0/1 Switchport: Enabled Administrative Mode: dynamic auto Operational Mode: static access Administrative Trunking Encapsulation: negotiate Operational Trunking Encapsulation: native Negotiation of Trunking: On Access Mode VLAN: 10 (VLAN0010) Trunking Native Mode VLAN: 1 (default) Administrative Native VLAN tagging: enabled Voice VLAN: none Administrative private-vlan host-association: none Administrative private-vlan mapping: none Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk Native VLAN tagging: enabled Administrative private-vlan trunk encapsulation: dot1q Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk associations: none Administrative private-vlan trunk mappings: none Operational private-vlan: none Trunking VLANs Enabled: ALL Pruning VLANs Enabled: 2-1001

▪ Puertos sin usar que se encuentran encendidos	
▪ Puertos sin uso en VLAN 1	
▪ No tiene “vlan dot1q tag native”	

Elaborado por: Pilamunga Norma, 2017

Detallamos a continuación las vulnerabilidades encontradas según el tipo de Ataque Switch Spoofing Tabla 4-3 y Double Tagging Tabla 5-3.

Tabla 4-3 Ataque 1: Switch Spoofing

Vulnerabilidades detectadas en el Escenario
DTP habilitado en los switch Cisco por defecto
Configuración automática de los trunk 802.1Q
Uso de la VLAN NATIVA (VLAN 1)
Puertos en no mode “access”
Pobre configuración de los puertos. (puertos troncales no configurados)
Puertos sin usar que se encuentran encendidos
Puertos sin uso en VLAN 1
Ausencia de políticas de seguridad
Nivel de conocimiento del atacante
Usuarios con prioridades dentro de la organización con privilegios y permisos
Falta de autentificación de usuarios, accesos no autorizados
Falta de monitorización de la red

Elaborado por: Pilamunga Norma, 2017

Tabla 5-3 Ataque 2: Double Tagging Vulnerabilidades detectadas en el Escenario
Configuración automática de los trunk 802.1Q
Puertos trunk presentes en la misma VLAN nativa que el atacante
Uso de la VLAN NATIVA (VLAN 1)
Pobre configuración de los puertos. (puertos troncales no configurados)
Puertos sin usar que se encuentran encendidos
Puertos sin uso en VLAN 1
No tiene “vlan dot1q tag native”
Ausencia de políticas de seguridad
Nivel de conocimiento del atacante
Usuarios con prioridades dentro de la organización con privilegios y permisos
Falta de autentificación de usuarios, accesos no autorizados
Falta de monitorización de la red

Elaborado por: Pilamunga Norma, 2017

3.8.3 Fase 3. Explotación de vulnerabilidades

Una vez identificadas las vulnerabilidades se persigue el control completo del mismo adquiriendo permisos y privilegios de los administradores, esta técnica se conoce como pivotar, es decir, saltar de un equipo a otro con la intención de controlar todos los equipos de la organización. (Díaz, 2014)

3.8.3.1 *Switch Spoofing*

El ataque se realiza desde la máquina atacante Kali Linux a través de la herramienta Yersinia. Gráfico 9-3

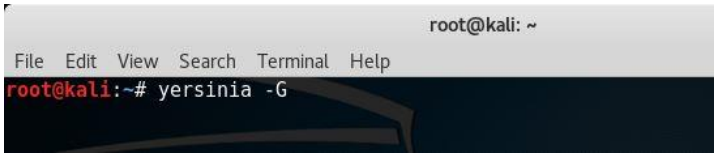


Gráfico 9-3 Ejecución de la herramienta Yersinia

Elaborado por: Pilamunga Norma, 2017

Desde la pestaña “802.1Q” o “DTP” Gráfico 10-3 se verifica que existan paquetes del tipo DTP, eso significa que el switch esté enviando este tipo de paquetes, como se muestra en el Gráfico 11-3

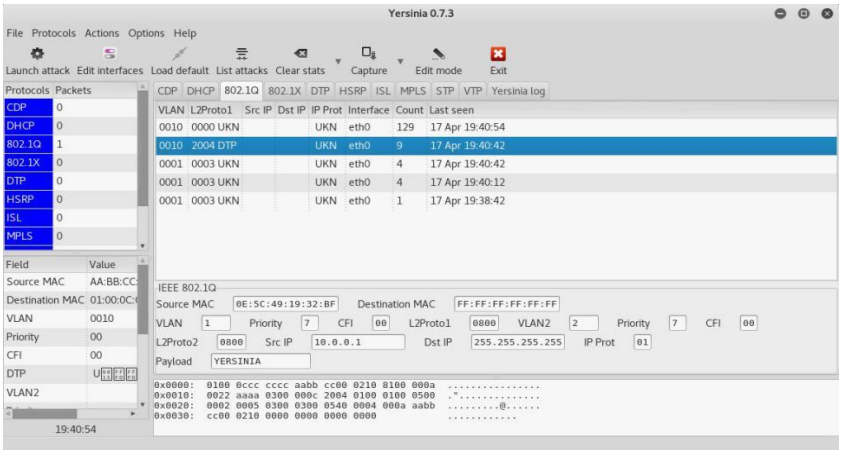


Gráfico 10-3 Captura de tráfico

Elaborado por: Pilamunga Norma, 2017

Como se puede observar en la imagen de arriba efectivamente existen mensajes DTP, lo que significa que se podrá realizar la negociación y transformar el puerto en trunk. Damos clic en el ícono "Launch attack" y elegimos "enabling trunking" y dar click en "OK" como se muestra en el Gráfico 12-3.

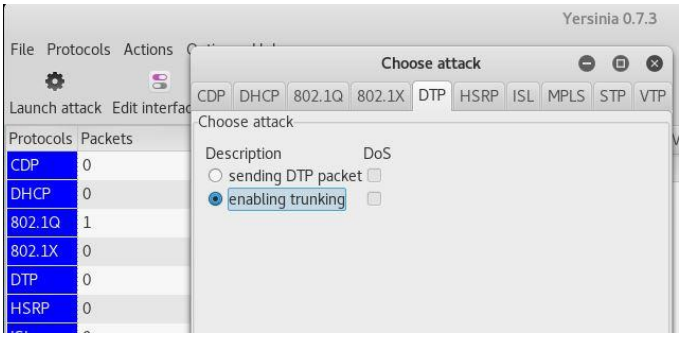


Gráfico 11-3 Captura de tráfico

Elaborado por: Pilamunga Norma, 2017

Se puede observar en la pestaña "DTP" Gráfico 12-3 que la interfaz eth0 está en estado "DESIRABLE".

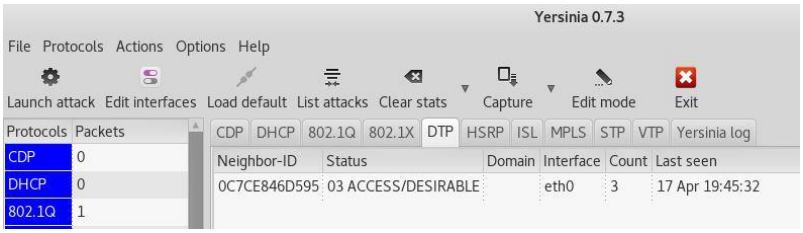


Gráfico 12-3 Estado Desirable

Elaborado por: Pilamunga Norma, 2017

Se debe comprobar en el Switch 1 que está el puerto Et0/1 en modo trunk, y efectivamente pasó de a modo trunk y la "n" en Encapsulation significa que fue negociado. Gráfico 13-3.

```
IOU1#sh interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et0/1       desirable        n-802.1q       trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et0/1       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,10,20,30
Et0/1       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10,20,30
Et0/1       1,10,20,30
```

Gráfico 13-3 Puerto Et0/1 en modo trunk

Elaborado por: Pilamunga Norma, 2017

Ahora que el puerto por donde está el atacante conectado se encuentra en modo trunk, se procede a saltar de VLANs. Para esta prueba se va a saltar a la VLAN 20. Gráfico 1-3. El primer paso es crear una VLAN en kali Linux:

- modprobe 8021q
- vconfig add eth0 20 (20 es la VLAN a la que se desea saltar)

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# modprobe 8021q
root@kali:~# vconfig add eth0 20
Added VLAN with VID == 20 to IF -:eth0:-
root@kali:~#
```

Gráfico 14-3 Creación de una VLAN en kali Linux

Elaborado por: Pilamunga Norma, 2017

Lo siguiente es crear una subinterfaz que pertenezca a la VLAN 20 Gráfico 15-3 y probar conexión con una PC con la VLAN 20. Gráfico 16-3.

- Ifconfig eth0.20 192.168.20.122/24 up

Donde eth0.20 es la VLAN a la que se debe conectar

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ifconfig eth0.20 192.168.20.122/24 up
root@kali:~# ifconfig eth0.20
eth0.20: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.122  netmask 255.255.255.0  broadcast 192.168.20.255
        inet6 fe80::20c:29ff:feef:ae14  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ef:ae:14  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 592 (592.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Gráfico 15-3 Creación de Subinterfaz

Elaborado por: Pilamunga Norma, 2017

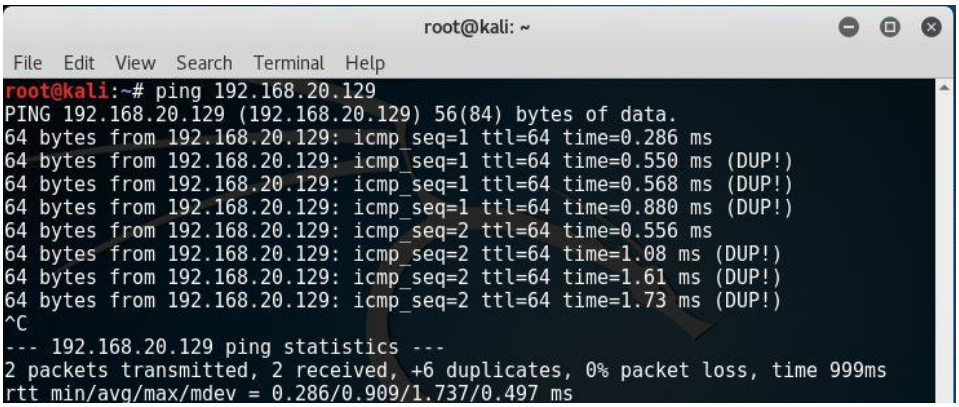


Gráfico 16-3 Prueba de conexión con la VLAN 20

Elaborado por: Pilamunga Norma, 2017

3.8.3.2 *Double Tagging*

Para este ataque se va a utilizar el mismo escenario anterior, por lo que solo se mostraran los resultados más no las con gráfico. Desde la máquina con kali Linux ejecutamos Yersinia. Y al seleccionar la pestaña “802.1Q” se observa que hay mensajes DTP. Gráfico 17-3.

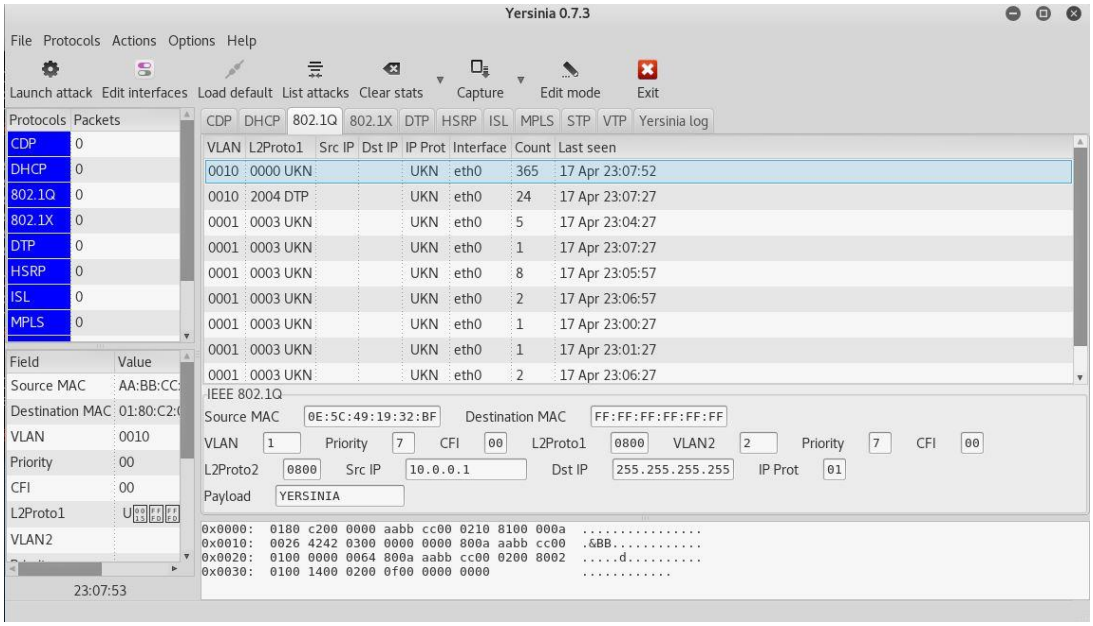


Gráfico 17-3 Prueba de conexión con la VLAN 20

Elaborado por: Pilamunga Norma, 2017

Luego de iniciar wireshark desde la consola Gráfico 18-3, se elige la interfaz que se vaya a usar para la captura, en este caso la “eth0” Gráfico 19-3 y se empieza la captura con el filtro “icmp”. Gráfico 20-3

Gráfico 18-3 Wireshark

Elaborado por: Pilamunga Norma, 2017

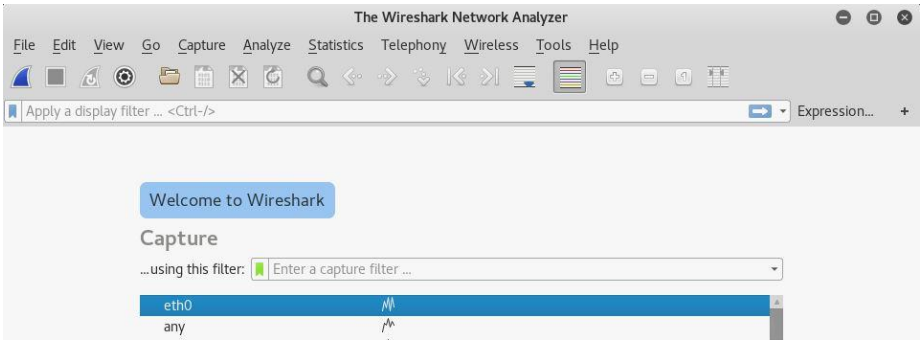


Gráfico 19-3 Wireshark, interfaz eth0

Elaborado por: Pilamunga Norma, 2017

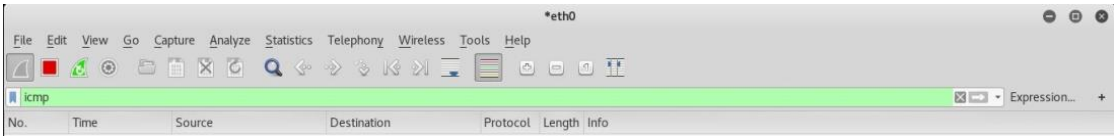


Gráfico 20-3 Wireshark, interfaz eth0, filtro ICMP

Elaborado por: Pilamunga Norma, 2017

A continuación, se lanza el ataque en Yersinia dando click en "Launch attack", en la ventana que se abre elegir "802.1Q" y ahí dar en la opción "sending 802.1Q double enc. paquets". Click en OK. Gráfico 21-3. Finalmente se puede ver en wireshark el paquete ICMP que envía Yersinia con etiqueta a dos VLAN diferentes. Gráfico 22-3.

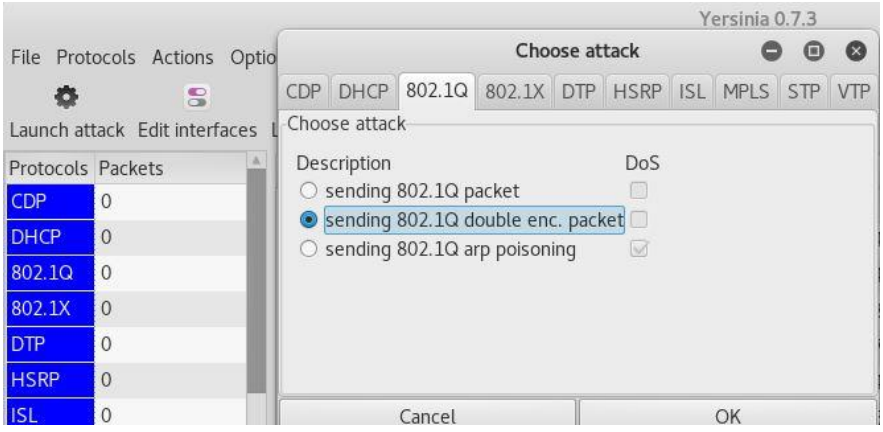


Gráfico 21-3 Ataque Double Tagging

Elaborado por: Pilamunga Norma, 2017

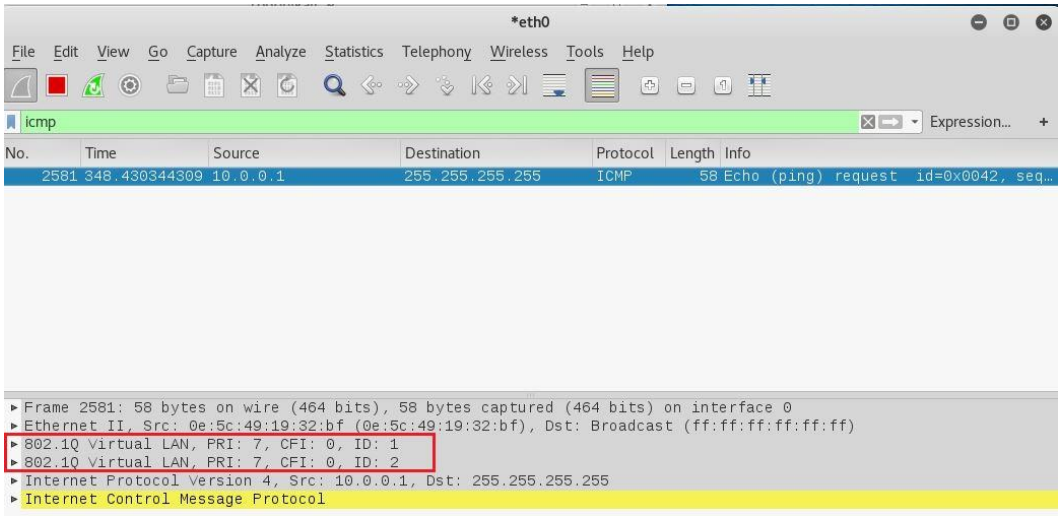


Gráfico 22-3 Etiquetas 802.1Q

Elaborado por: Pilamunga Norma, 2017

La primera etiqueta esta para la VLAN 1. Gráfico 23-3

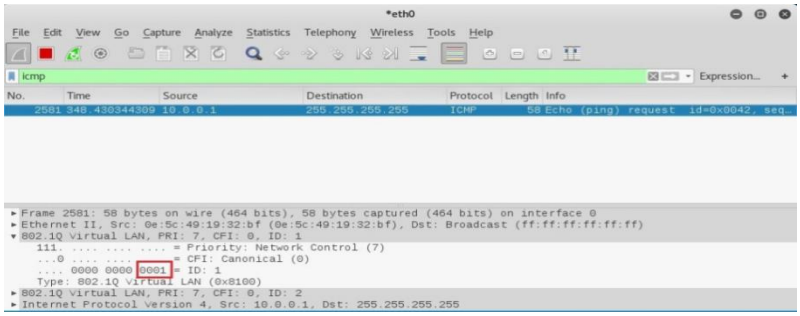


Gráfico 23-3 Primera Etiqueta 802.1Q

Elaborado por: Pilamunga Norma, 2017

Y la segunda etiqueta es para la VLAN 10. Gráfico 25-3

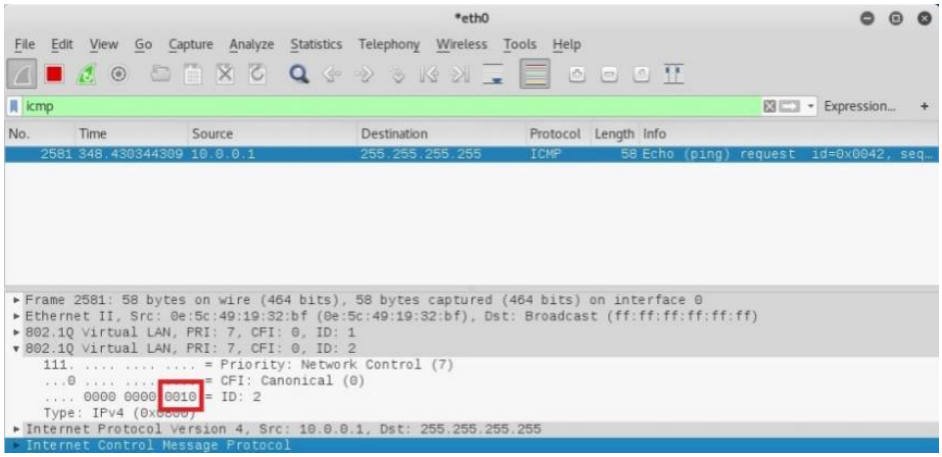


Gráfico 24-3 Segunda Etiqueta 802.1Q

3.8.4 Fase 4. Informe

Finalmente tenemos que presentar el resultado de la auditoría a la infraestructura de red, de manera que este comprenda la seriedad de los riesgos emanantes de las vulnerabilidades descubiertas, remarcando aquellos puntos en los que la seguridad se había implantado de manera correcta y aquellos que deben ser corregidos.

Como posiblemente este informe sea leído tanto por personal de IT como por responsables sin conocimientos técnicos conviene separar el informe en una parte de explicación general y en otra parte más técnica lo que vendría a ser por una parte el informe ejecutivo y el informe técnico.

Lo más importante en este tema de investigación específicamente son las Políticas de Seguridad que consisten en recomendaciones y contramedidas para mitigar las vulnerabilidades de los Ataques VLAN HOPPING. Estás políticas de seguridad son tecnológicas es decir de implementación y organizacionales con el fin de mejorar las acciones por parte de los administradores de red y de educar a los usuarios.

3.9 Planteamiento de la Hipótesis

3.9.1 Hipótesis de Investigación

Hi: ¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitiga luego de la aplicación de las Políticas de Seguridad propuestas?

3.9.2 Hipótesis Nula

Ho: ¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mantienen luego de la aplicación de las Políticas de Seguridad propuestas?

3.10 Determinación de variables

3.10.1 Operacionalización Conceptual

La Tabla 6-3 muestra la operacionalización conceptual de las variables determinadas.

Tabla 6-3 Operacionalización conceptual

VARIABLE	TIPO	CONCEPTO
Vulnerabilidades de los ataques VLAN HOPPING	Independiente	Las vulnerabilidades de los ataques VLAN HOPPING son debilidades, errores de configuración en la infraestructura de red, que permite al atacante realizar desde dentro de la red un salto de VLAN logrando acceso sin permiso del administrador de red.
Políticas de Seguridad	Dependiente	Son un conjunto de normas, reglas de seguridad que permiten definir procedimientos necesarios para controlar y minimizar vulnerabilidades de infraestructura de red.

Elaborado por: **Pilamunga Norma, 2017**

3.10.2 Operacionalización Metodológica

La Tabla 7-3, muestra la operacionalización metodológica de las variables independiente y dependiente.

HIPÓTESIS GENERAL	VARIABLES		INDICADORES	INDICES	TÉCNICAS	INSTRUMENTOS
¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitigan luego de la aplicación de las Políticas de Seguridad propuestas?	INDEPENDIENTE	Vulnerabilidades de los ataques VLAN HOPPING	▪ Protocolo habilitado ▪ Configuraciones por defecto de los puertos del switch ▪ Configuraciones incorrectas de los puertos trunk ▪ Suplantación de switch ▪ Puertos abiertos de switch sin uso	✓ DTP habilitado en los switch Cisco por defecto ✓ Configuración automática de los trunk 802.1Q ✓ Uso de la VLAN NATIVA (VLAN 1) ✓ Puertos de acceso en no modo "Access" ✓ Puertos sin uso habilitados ✓ No tiene "vlan dot1q tag native"	▪ Búsqueda de información ▪ Observación ▪ Pruebas	▪ GN3: Emulador ▪ Kali linux ▪ Yersinia: Software para vulnerabilidades ▪ Wireshark
	DEPENDIENTE	Políticas de Seguridad	▪ Ausencia de políticas de seguridad ▪ Nivel de conocimiento del atacante ▪ Usuarios con prioridades dentro de la organización con privilegios y permisos ▪ Falta de autentificación de usuarios, accesos no autorizados ▪ Falta de monitorización de la red	✓ Seguridad de la Información ✓ Seguridad relativa a los recursos humanos: a. Entrenamiento b. Capacitación al personal técnico y al usuario final ✓ Control de acceso físico al data center ✓ Seguridad física y del Entorno ✓ Seguridad de las comunicaciones a. Monitorización de la red ✓ Gestión de incidentes de seguridad de la información ✓ Cumplimiento	▪ Búsqueda de información ▪ Encuesta ▪ Observación ▪ Pruebas	

Elaborado por: **Pilamunga Norma, 2017**

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En este capítulo se analizan y comparan los resultados de los ataques VLAN HOPPING obtenidos en las pruebas ejecutadas en el escenario de prueba implementado en GNS3 sin y con políticas de seguridad para finalmente comprobar la hipótesis planteada.

4.1 Presentación de resultados

Luego de explotar las vulnerabilidades encontradas, se observa los resultados de los ataques VLAN HOPPING ejecutados en el ambiente de pruebas sin políticas de seguridad y con políticas de seguridad.

4.1.1 Resultados sin políticas de seguridad

El atacante se encuentra conectado al Switch 1 y a la Vlan 10 como se observa en el Gráfico 1-4, por lo que las condiciones fue enfocada desde el punto de vista del atacante.

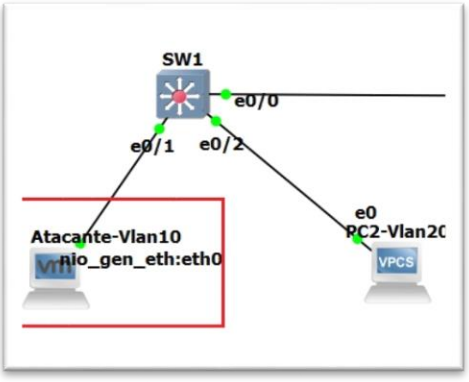


Gráfico 1-4 Atacante conectado

Elaborado por: **Pilamunga Norma, 2017**

Una vez lanzado el ataque desde Yersinia se concreta la negociación y se establece el enlace troncal. Haciendo un ping se comprueba que se obtiene éxito como se muestra en el Gráfico 2-4.

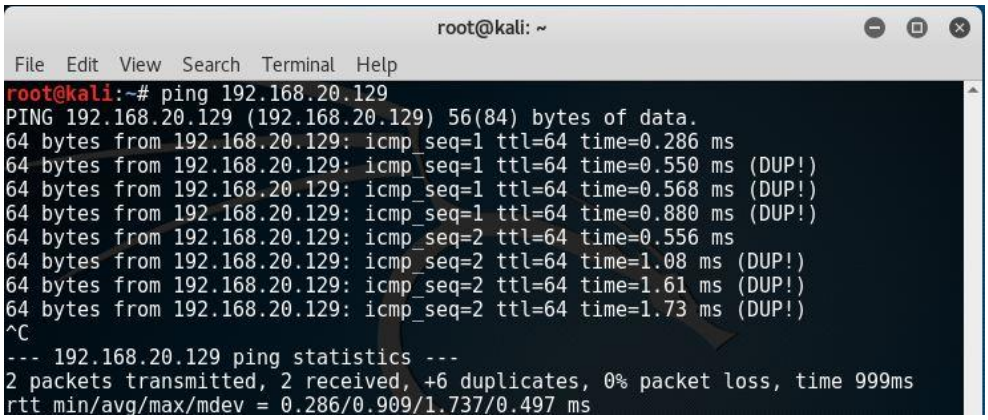


Gráfico 2-4 Comprobación Ping desde la máquina Atacante con la sub interfaz de la VLAN 20

Elaborado por: **Pilamunga Norma, 2017**

En la tabla 1-4 se resume el éxito al explotar todas las vulnerabilidades encontradas con el Ataque 1: Switch Spoofing.

Tabla 1-4 Éxito de explotación de vulnerabilidades Ataque 1: Switch Spoofing

Vulnerabilidades detectadas	SI	NO
DTP habilitado en los switch Cisco por defecto	X	
Configuración automática de los trunk 802.1Q	X	
Uso de la VLAN NATIVA (VLAN 1)	X	
Puertos en no mode “access”	X	
Pobre configuración de los puertos. (puertos troncales no configurados)	X	
Puertos sin usar que se encuentran encendidos	X	
Puertos sin uso en VLAN 1	X	
Ausencia de políticas de seguridad	X	
Nivel de conocimiento del atacante	X	
Usuarios con prioridades dentro de la organización con privilegios y permisos	X	
Falta de autentificación de usuarios, accesos no autorizados	X	
Falta de monitorización de la red	X	

Elaborado por: Pilamunga Norma, 2017

Así mismo en la tabla 2-4 se explota las vulnerabilidades del Ataque Double Tagging.

Tabla 2-4 Explotación de vulnerabilidades Ataque 2: Double Tagging

Vulnerabilidades detectadas	SI	NO
Configuración automática de los trunk 802.1Q	X	
Puertos trunk presentes en la misma VLAN nativa que el atacante	X	
Uso de la VLAN NATIVA (VLAN 1)	X	
Pobre configuración de los puertos. (puertos troncales no configurados)	X	
Puertos sin usar que se encuentran encendidos	X	
Puertos sin uso en VLAN 1	X	
No tiene "vlan dot1q tag native"	X	
Ausencia de políticas de seguridad	X	
Nivel de conocimiento del atacante	X	
Usuarios con prioridades dentro de la organización con privilegios y permisos	X	
Falta de autentificación de usuarios, accesos no autorizados	X	
Falta de monitorización de la red	X	

Elaborado por: Pilamunga Norma, 2017

La falta de políticas de seguridad dentro de una organización se convierte en un problema para los administradores de red que no entienden las desventajas de dejar sus puertos con configuraciones por defecto. Según los resultados obtenidos se observa que sin políticas puedo vulnerar la red usando Switch Spoofing o Double Tagging obteniendo acceso al sistema sin dificultad.

4.1.2 Resultados con políticas de seguridad

Para esta sección aplicamos las políticas de seguridad definidas de acuerdo a las vulnerabilidades detectadas.

4.1.2.1 *Políticas de Seguridad para evitar Ataque Switch Spoofing*

1. **Política 1: No usar VLAN nativa 1 en los puertos trunk. Colocar los puertos de acceso en modo Access**, las configuraciones se detallan en el Anexo 5, básicamente se crea la VLAN 99 y se reemplaza la VLAN Nativa 1, luego los puertos de acceso se colocan en modo Access y se lanza el ataque obteniendo éxito como se muestra en el Gráfico 3-4.

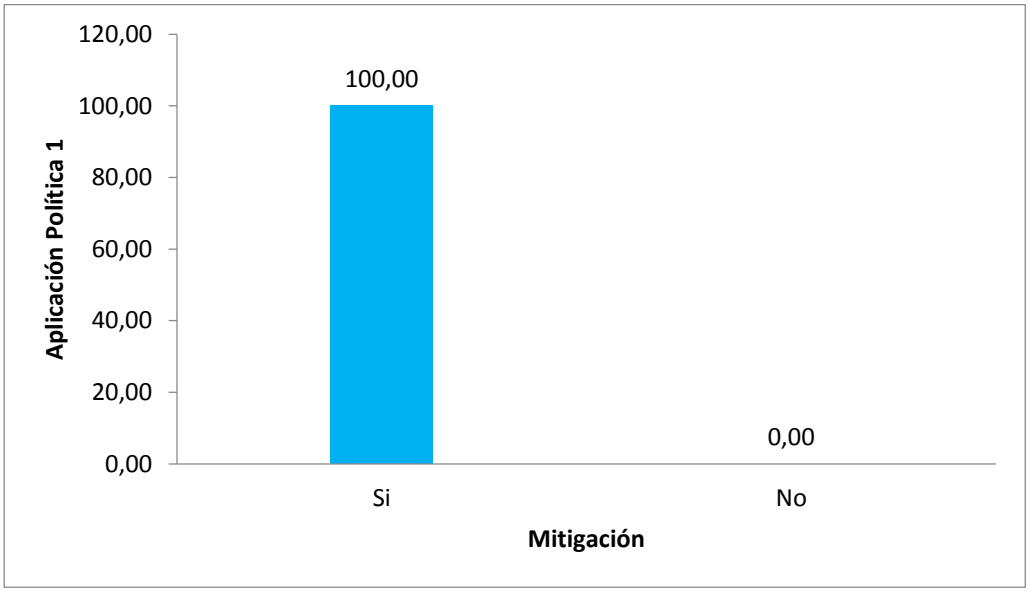


Gráfico 3-4 Política 1

Elaborado por: Pilamunga Norma, 2017

Según los datos obtenidos se puede observar que con la aplicación de la Política 1, se logró en un 100% mitigar las vulnerabilidades es decir al proteger la VLAN nativa se evita que sea ocupada para usos administrativos, igualmente se complementa con la configuración de los puertos en modo Access.

2. **Política 2: Crear una VLAN XY, poner a todos los puertos sin uso a la VLAN XY y declarar estos puertos sin uso en modo "Access", las configuración se muestran en el Anexo 6,** se crea la VLAN XY y se complementa configuración los puertos sin uso en modo Access. En el Gráfico 4-4, se muestra el éxito de la aplicación de esta política.

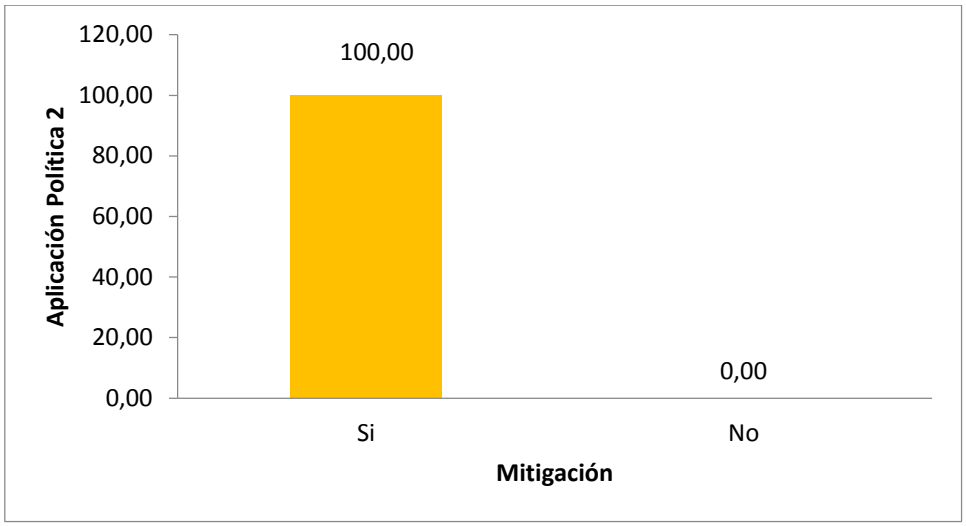


Gráfico 4-4 Política 2

Elaborado por: Pilamunga Norma, 2017

Según los datos obtenidos se puede observar que con la aplicación de la Política 2, se logró el 100% de mitigación de las vulnerabilidades es decir al configurar el switch creamos la VLAN 999 con el nombre de XY, seleccionamos el rango de puertos y colocamos en modo Access.

3. **Política 3: Poner los puertos de acceso en modo "Access",** se selecciona el rango de puertos a ser configurar como modo Access y se verifica como se muestra en la Gráfico 5-4.

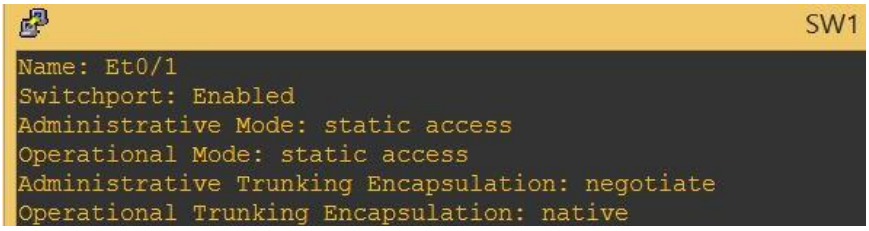


Gráfico 5-4 Verificación Política 3

Elaborado por: Pilamunga Norma, 2017

A continuación se muestra en el Gráfico 6-4 el éxito de la aplicación de la política 3.

Gráfico 6-4 Política 3

Elaborado por: Pilamunga Norma, 2017

En la gráfica se observa que al aplicar la política 3 se obtiene el 100 % de éxito de mitigación del ataque Switch Spoofing, esto se debe a que si se configura como modo Access los puertos solo transportarán tráfico de una sola VLAN.

4. Política 4: Deshabilitar DTP (Ver Anexo 7)

Para deshabilitar DPT se hace uso del comando no negotiate que solo funciona en puertos troncales y en modo Access. Grafico 7-4

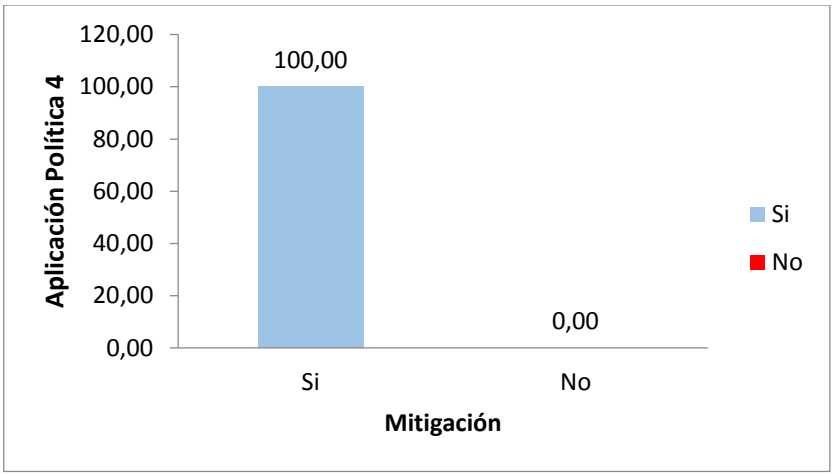


Gráfico 7-4 Política 4

Elaborado por: Pilamunga Norma, 2017

Como podemos observar se mitiga al 100% esta vulnerabilidad, es quizá el problema más relevante al que se enfrenta el administrador de red cuando por falta

de experticia originamos vulnerabilidades que pueden afectar gravemente el óptimo desempeño de la red como es el caso del protocolo DTP de CISCO.

5. **Política 5: Apagar todos los puertos no utilizados con el comando Shutdown y los puertos de acceso en modo Access,** en nuestro escenario si el atacante se conecta en el puerto apagado como el et1/0 Gráfico 8-4.

```
IOU1(config)#int rang e1/0 -3
IOU1(config-if-range)#shu
IOU1(config-if-range)#shutdown
IOU1(config-if-range)#
```

Gráfico 8-4 Política 5

Elaborado por: Pilamunga Norma, 2017

En el siguiente Gráfico 9-4 se observa el éxito de la aplicación de la política 5.

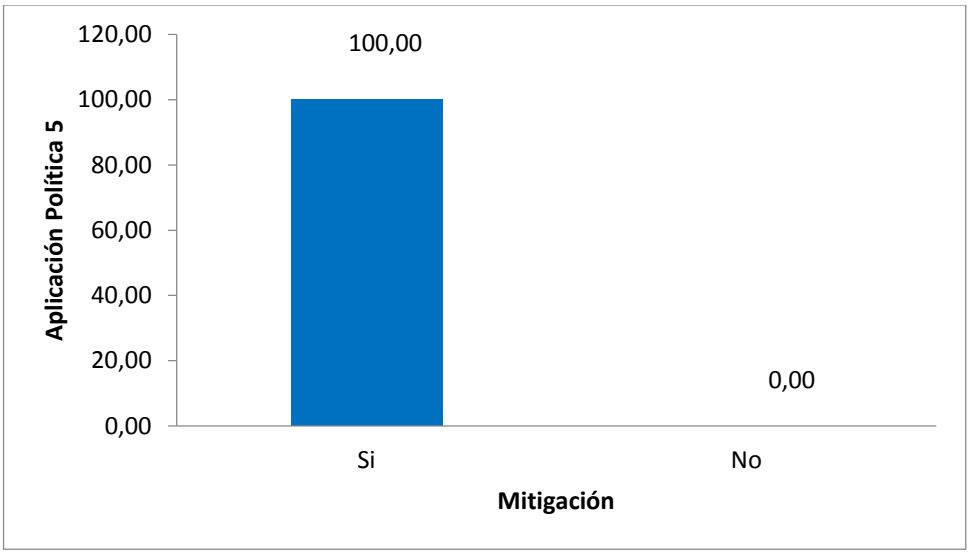


Gráfico 9-4 Política 5: Apagar puertos no utilizados con el comando shutdown

Elaborado por: Pilamunga Norma, 2017

Apagar todos los puertos no utilizados con el comando shutdown, asegura el 100% de éxito de mitigación pues es el método más simple que los administradores usan para contribuir a la seguridad de la red ante accesos no autorizados, esto es inhabilitar todos los puertos del switch que no se utilizan.

4.1.2.2 *Políticas de Seguridad para evitar Double Tagging*

1. **Política 1:** No asignar ningún puerto a la Vlan 1. Al igual que la Política 1 Switch Spoofing
2. **Política 2:** No usar la VLAN nativa 1. Al igual que la Política 2 Switch Spoofing.
3. **Política 3: Etiquetado explícito de la VLAN nativa en todos los puertos trunk. Debe configurarse en todos los switch de la red.**

Se comprueba que al aplicar la política Grafico 10-4, no permite el ataque y se mitiga la vulnerabilidad.

```
IOU1(config)#vlan dot1q tag native
IOU1(config)#
```

Gráfico 10-4 Comprobación Política 3 Double Tagging

Elaborado por: Pilamunga Norma, 2017

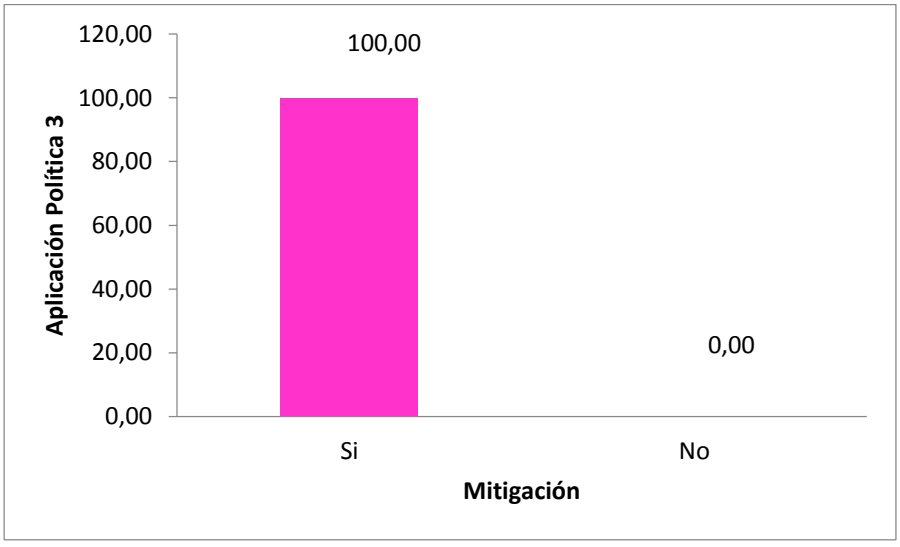


Gráfico 11-4 Política 3 Double Tagging

Elaborado por: Pilamunga Norma, 2017

Al igual que todas las políticas se observa que obtenemos el 100% de éxito de mitigación al habilitar el etiquetado dot1q (IEEE 802.1Q) para todas las VLAN nativas en todos los puertos troncales del switch.

4. Poner los puertos de acceso en modo “Access” al igual que la Política 3 Switch Spoofing.

Todas las políticas han sido probadas y se comprueba que no podemos ejecutar VLAN HOPPING, al ejecutar Yersinia se observa que ya no existen mensajes de DTP Grafico 12-4 y Grafico 13-4, por lo que ya no ejecuta la negociación, además que el puerto del switch 1 e0/1 ya no se hace troncal.

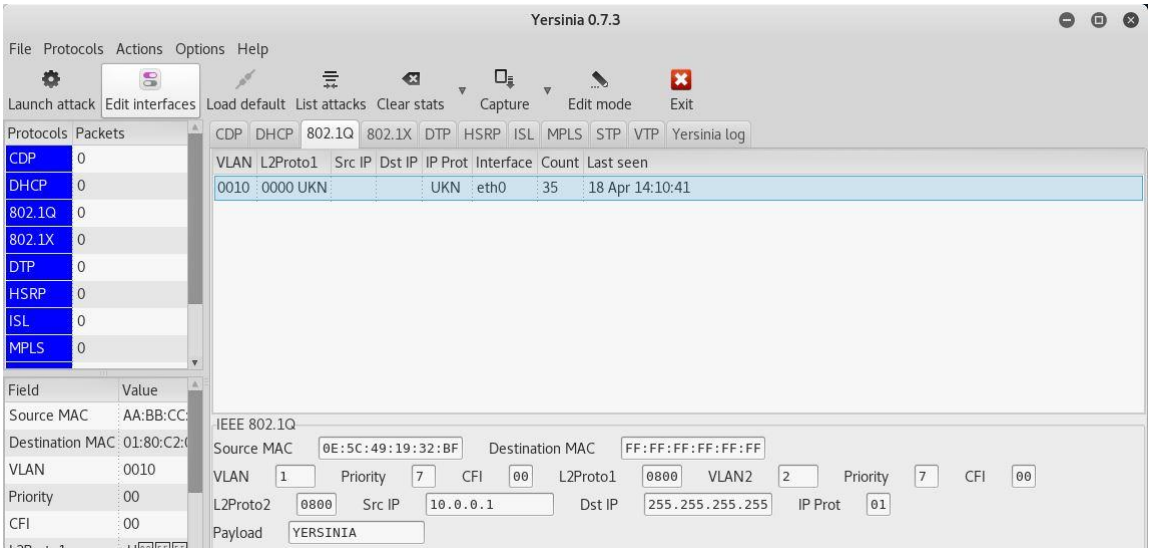


Gráfico 12-4 Comprobación de políticas de seguridad

Elaborado por: Pilamunga Norma, 2017

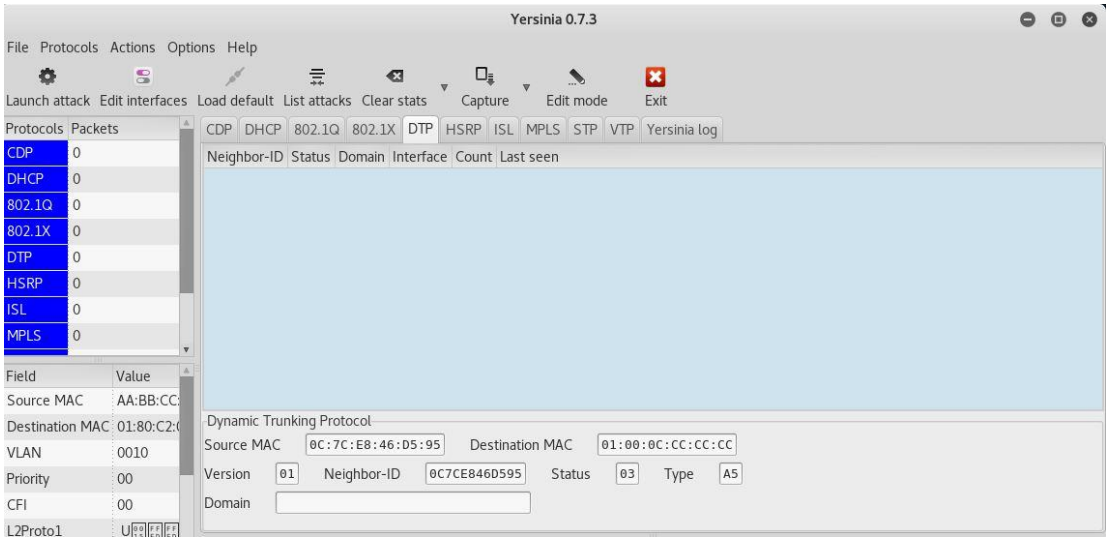


Gráfico 13-4 Verificación de la no existencia de mensajes de DTP

Elaborado por: Pilamunga Norma, 2017

Se vuelve a lanzar el ataque de igual manera que en el caso de práctica y se comprueba en el switch que el puerto et0/1 ya no se hace trunk. Grafico 14-4.

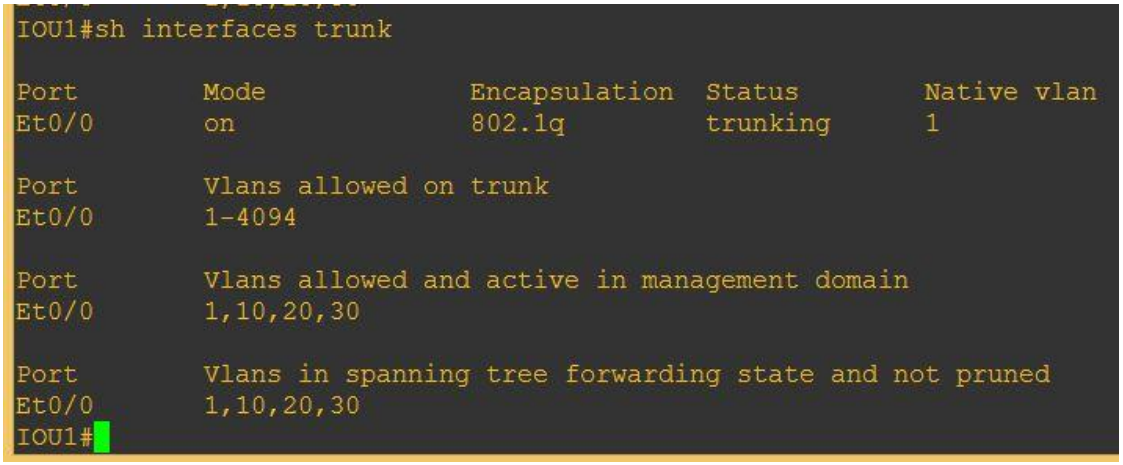


Gráfico 14-4 Verificación de que ya no es posible el Ataque

Elaborado por: Pilamunga Norma, 2017

4.2 Análisis e interpretación de resultados

Una vez realizadas las pruebas en el escenario establecido con y sin políticas de seguridad, se procede con el análisis, comparación e interpretación de los resultados obtenidos al ejecutar los ataques Switch Spoofing y Double Tagging, conjuntamente las políticas y sus vulnerabilidades. Tabla 3-4

Tabla 3-4 **Análisis de vulnerabilidades VLAN HOPPING y políticas**

Vulnerabilidades / Políticas	Tecnológicas								Organizacionales, Operacionales Y Físicas						
	DTP Activado	VLAN nativa 1	Puertos en no mode "Access"	Puertos sin usar que se encuentran encendidos	Puertos sin uso en VLAN 1	No tiene activado "vlan dot1q tag native"	Configuración automática de los trunk 802.1Q	TOTAL	Pobre configuración de los puertos	Ausencia de políticas de seguridad	Nivel de conocimiento alto del atacante interno	Usuarios con prioridades dentro de la organización	Accesos no autorizados	Falta de monitorización de la red	TOTAL
No usar VLAN nativa 1 en los puertos trunk. Colocar los puertos de acceso en modo access.	0,000	1,000	0,000	0,000	0,000	0,000	1,000	2,000	0,167	0,167	0,167	0,167	0,167	0,167	1,000
Crear una VLAN XY, poner a todos los puertos sin uso a la VLAN XY, declarar estos puertos sin uso en modo "Access"	0,000	0,000	0,000	0,000	1,000	0,000	0,000	1,000	0,167	0,167	0,167	0,167	0,167	0,167	1,000
Poner los puertos de acceso en modo "Access"	0,000	0,000	1,000	0,000	0,000	0,000	0,000	1,000	0,167	0,167	0,167	0,167	0,167	0,167	1,000
Deshabilitar DTP: Nunca dejar un puerto de acceso en modo "Dynamic Desirable ", "Auto Dynamic" o "Trunk".	1,000	0,000	0,000	0,000	0,000	0,000	0,000	1,000	0,167	0,167	0,167	0,167	0,167	0,167	1,000
Apagar todos los puertos no utilizados con el comando shutdown y colocar los puertos de acceso en modo access.	0,000	0,000	0,000	1,000	0,000	0,000	0,000	1,000	0,167	0,167	0,167	0,167	0,167	0,167	1,000
Etiquetado explícito de la VLAN nativa en todos los puertos trunk. Debe configurarse en todos los switches de la red.	0,000	0,000	0,000	0,000	0,000	0,000	1,000	1,000	0,167	0,167	0,167	0,167	0,167	0,167	1,000
	1,000	1,000	1,000	1,000	1,000	0,000	2,000	7,000	1,000	1,000	1,000	1,000	1,000	1,000	6,000

Elaborado por: Pilamunga Norma, 2017

4.3 Prueba de la hipótesis de investigación

4.3.1 Hipótesis de Investigación

¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitigan luego de la aplicación de las Políticas de Seguridad propuestas?

4.3.2 Objetivo

- Proponer buenas prácticas o guía para mitigar las vulnerabilidades de los ataques VLAN HOPPING en la capa de enlace de datos, a partir de la implantación de políticas de seguridad con perfecta claridad y transparencia en la organización.

4.3.3 Resultados de indicadores

La medición del indicador, se realiza por el número de vulnerabilidades encontradas, se muestra en la Tabla 4-4, en la que se lista las vulnerabilidades encontradas en el escenario de pruebas, donde se determina si fue posible la mitigación después de aplicar las Políticas de Seguridad.

Tabla 4-4 Análisis de resultados de Mitigación de vulnerabilidades VLAN HOPPING

	Vulnerabilidades VLAN HOPPING	Se mitigó?	
1.	DTP habilitado en los switch Cisco por defecto	SI	
2.	Configuración automática de los trunk 802.1Q	SI	
3.	Uso de la VLAN NATIVA (VLAN 1)	SI	
4.	Puertos en no mode “access”	SI	
5.	Pobre configuración de los puertos. (puertos troncales no configurados)	SI	
6.	Puertos sin usar que se encuentran encendidos	SI	
7.	Puertos sin uso en VLAN 1	SI	
8.	No tiene activado “vlan dot1q tag native”	SI	
9.	Ausencia de políticas de seguridad	SI	
10.	Nivel de conocimiento del atacante	SI	
11.	Usuarios con prioridades dentro de la organización con privilegios y permisos	SI	
12.	Falta de autentificación de usuarios, accesos no autorizados	SI	
13.	Falta de monitorización de la red	SI	
Total		13	0

Elaborado por: Pilamunga Norma, 2017

Se concluye entonces que mediante la implementación de las Políticas de Seguridad se mitiga las 13 vulnerabilidades de los Ataques VLAN HOPPING es decir se cumple con el 100% de éxito como se muestra en la Tabla 5-4 y se muestra el Gráfico 15-4.

Tabla 5-4 Mitigación de vulnerabilidades VLAN HOPPING

Políticas de Seguridad	Nro. de Vulnerabilidades encontradas
Sin políticas de seguridad	13
Con políticas de seguridad	0

Elaborado por: Pilamunga Norma, 2017

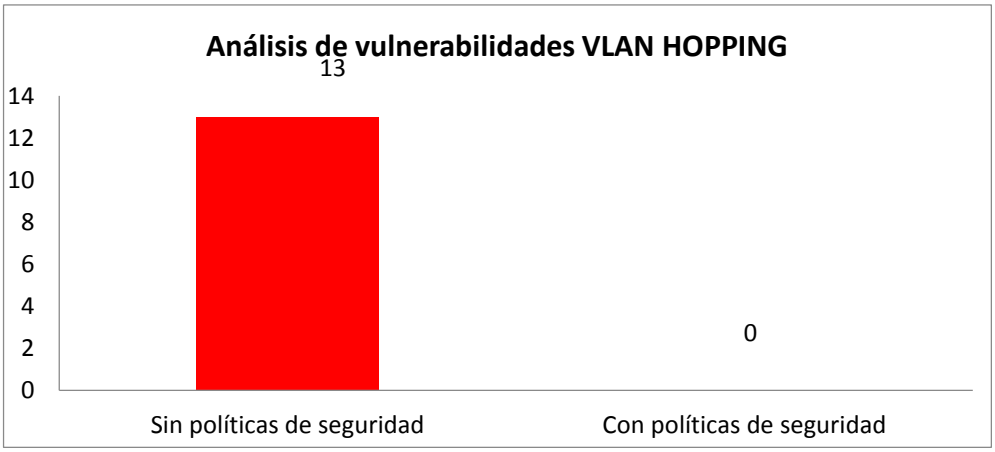


Gráfico 15-4 Análisis de vulnerabilidades VLAN HOPPING

Elaborado por: Pilamunga Norma, 2017

4.4 Comprobación estadística de la hipótesis

Se considera la Hipótesis de Investigación Hi y la Hipótesis Nula:

Hi: ¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitigan luego de la aplicación de las Políticas de Seguridad propuestas?

Ho: ¿Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mantienen luego de la aplicación de las Políticas de Seguridad propuestas?

A continuación un resumen de las políticas y vulnerabilidades mitigadas de la Tabla 3-4, a partir de la cual se colocan los resultados obtenidos para realizar la comprobación de la hipótesis y se agrupa las vulnerabilidades tecnológicas y las vulnerabilidades organizacionales, operacionales y físicas en la Tabla 6-4.

Tabla 6-4 Políticas y vulnerabilidades tecnológicas y las vulnerabilidades organizacionales, operacionales y físicas	**Vulnerabilidades**		**Total de mitigación de vulnerabilidades**
Políticas	Tecnológicas	Organizacionales, Operacionales Y Físicas	
No usar VLAN nativa 1 en los puertos trunk. Colocar los puertos de acceso en modo access.	2	1	3
Crear una VLAN XY, poner a todos los puertos sin uso a la VLAN XY, declarar estos puertos sin uso en modo “Access”	1	1	2
Poner los puertos de acceso en modo “Access”	1	1	2
Deshabilitar DTP: Nunca dejar un puerto de acceso en modo "Dynamic Desirable ", "Auto Dynamic" o "Trunk".	1	1	2
Apagar todos los puertos no utilizados con el comando shutdown y colocar los puertos de acceso en modo access.	1	1	2
Etiquetado explícito de la VLAN nativa en todos los puertos trunk. Debe configurarse en todos los switches de la red.	1	1	2
	7	6	13

Estadísticos descriptivos					
	N	Media	Desviación típica	Mínimo	Máximo
Tecnológicas	7	1,17	0,408	1	2
Organizacionales, Operacionales Y Físicas	6	1,00	0,000	1	1

Prueba de los rangos con signo de Wilcoxon

Rangos				
	N	Rango promedio		Suma de rangos
Organizacionales, Operacionales Y Físicas- Tecnológicas	Rangos negativos	1a	1,00	1,00
	Rangos positivos	0b	0,00	0,00
	Empates	5c		
	Total	6		

a. Organizacionales, Operacionales Y Físicas < Tecnológicas

b. Organizacionales, Operacionales Y Físicas > Tecnológicas

c. Organizacionales, Operacionales Y Físicas = Tecnológicas

Estadísticos de contraste b	
	Organizacionales, Operacionales Y Físicas - Tecnológicas
Z	-1,000a
Sig. asintót. (bilateral)	0,317
a. Basado en los rangos positivos.	
b. Prueba de los rangos con signo de Wilcoxon	

El valor p es mayor que el nivel de significancia 0,05 por lo tanto aceptamos H1 y concluimos que: Las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitigan luego de la aplicación de las políticas de seguridad propuestas.

CAPÍTULO V

5. PROPUESTA

Hoy el tema de la seguridad informática debe ser catalogado como prioritario y emergente, es importante que el personal técnico de las entidades públicas y privadas sea capacitado en esta área, hoy en Ecuador ya existe un número de profesionales pero su porcentaje sigue siendo bajo con respecto a los demás países en vías de desarrollo. Este cambio en la cultura informática en las organizaciones hará que el Departamento de Tecnologías de la Información y Comunicaciones TIC sea tomado en cuenta y conjuntamente con la Directiva se tomen acciones en pro de los objetivos de la organización.

Con la investigación sobre los ataques VLAN HOPPING se determina que la red LAN no es segura, para contrarrestar es necesario aplicar los correctivos dado que el principal enemigo se encuentra dentro de la misma organización por las prioridades y permisos con los que cuenta para acceder libremente por toda la organización incluso tener accesos a datos de carácter confidencial.

Esto hace que se proponga un documento de directrices que orienten el buen uso de estas recomendaciones para evitar el uso indebido de las mismas. Es entonces necesaria una herramienta organizacional como son las políticas de seguridad para concienciar al personal administrativo, técnicos, usuarios, invitados sobre la seguridad de la información.

Este documento principalmente hace referencia a lo que debe hacer un administrador de red para asegura su infraestructura de red frente a los ataques VLAN HOPPING.

Estas políticas de seguridad se centra en la configuración adecuada de los switches CISCO y se ha dividido las políticas en dos partes fundamentales la primera haciendo referencia a la mitigación de las vulnerabilidades de los Ataques VLAN HOPPING en

términos tecnológicos y la segunda parte dirigido a minimizar las vulnerabilidades Organizacionales, Operacionales y Físicas que están relacionadas.

5.1 Políticas de seguridad para mitigar las vulnerabilidades de los ataques VLAN HOPPING en la capa de enlace de datos.

5.1.1 Introducción

El Departamento de Tecnologías de la Información y Comunicaciones de la organización, será el encargado del proceso de implementación de las políticas de seguridad en relación a mitigar las vulnerabilidades de la Capa de Enlace de Datos a través de los ataques VLAN HOPPING y realizar las revisiones y mejoras a las mismas.

El propósito es hacer frente a un ataque VLAN HOPPING haciendo uso de la documentación adecuada para enfrentar estas amenazas resultado de tener una pobre configuración y que causan malestar en el desempeño de las actividades de toda organización.

5.1.2 Objetivos Específicos

- Proteger los equipos tecnológicos aplicando Políticas de Seguridad de acuerdo a las necesidades que genere la red.
- Establecer un esquema de seguridad para asegurar la confiabilidad, disponibilidad e integridad de la información de la infraestructura de red, protegiendo la tecnología de seguridad VLAN, frente a amenazas internas sean estas deliberadas o accidentales
- Implementar las políticas de seguridad para asegurar funcionamiento antes, durante y después de los ataques VLAN HOPPING.
- Documentar y mejorar las políticas de seguridad implementadas para mitigar ataques VLAN HOPPING

5.1.3 Alcance

Este manual de políticas de seguridad se define para gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico frente la pobre configuración frente a ataques VLAN HOPPING. Este documento va dirigido a todo el personal interno y externo de la organización, ya sea que cuente con una infraestructura de red pequeña o extensa. Se proporciona lineamientos que mejoran, recuperan y protegen la red LAN cuando un recurso está siendo amenazado.

5.1.4 Definiciones

En esta sección del documento se presenta los términos utilizados en este documento de políticas de seguridad.

- **Activo**: Cualquier cosa que tenga valor para la organización.
- **Amenaza**: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.
- **Ataque**: Intento de penetración a una red por parte de un usuario no deseado ni autorizado.
- **Buen uso**: se entiende por "buen uso" al cuidado de los activos por parte del personal.
- **Comité de Seguridad**: equipo formado por los jefes que representan a las áreas de la organización, responsable de la toma de decisiones en temas de la seguridad de la información.
- **Confidencialidad:** asegurar que la información sea accesible sólo a las personas autorizadas
- **Cuarto de Comunicación**.- Área dedicada al alojamiento exclusivo de equipos informáticos asociado al cableado de telecomunicaciones.
- **Disponibilidad:** asegurar que los activos o información puedan ser utilizados en cualquier momento
- **Hacking ético:** es el conjunto de actividades para ingresar a las redes de datos y voz dentro de las organizaciones con el propósito de lograr de forma controlada ataques sin ninguna intensión criminal sino con el objetivo de proponer acciones correctivas para mejorar el nivel de seguridad.
- **Integridad:** es salvaguardar la exactitud de la información en su procesamiento, transmisión y almacenamiento.

- **Inventario de activos:** es una lista ordenada y documentada de los activos de la organización.
- **Perfiles de usuario**: son grupos que agrupan a usuarios según funciones similares sobre permiso de uso de los recursos tecnológicos o los sistemas de información.
- **Personal:** toda persona que tiene autorización para acceder a la información, sea interna o externa a la organización.
- **Política**: El estándar define que se deben constituir las políticas de seguridad donde se documenten los procedimientos internos de la organización, reflejando las expectativas en materia de seguridad, las cuales deben servir de soporte para el comité de seguridad que revisa y actualiza dichos procedimientos.
- **Recursos tecnológicos:** Componentes de hardware: servidores de aplicaciones, servidores de servicios de red, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad como switches, router, Access point, servicios de red de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.
- **Seguridad de la Información:** es la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información. Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confiabilidad.
- **SGI:** Sistema de Gestión de Inventarios
- **Supervisor:** persona responsable del departamento de tecnologías y comunicaciones.
- **Usuario**: Entidad o individuo que utiliza un sistema
- **Usuarios Terceros**: Personas naturales o jurídicas, que no son funcionarios de la organización, pero que requieren tener acceso a los recursos informáticos para llevar a cabo determinada actividad.
- **Vulnerabilidades:** son los huecos de seguridad resultado de una pobre configuración que involucran a los activos que pueden ser explotadas desde dentro de la infraestructura de red.

5.1.5 Usuarios a los que va dirigido

- Dirigida al Gerente o Director de la Organización quien como cabeza debe propender a cuidar de los activos (información y recursos, dispositivos de red) de la organización y aplicar herramientas que permitan lograr este objetivo.
- Departamento de Tecnologías de Información y Comunicaciones. Administradores de red o personal técnico con conocimiento específico en configuraciones de servidores, switches, router, levantamiento de servidores, entre otros aspectos relacionados con la seguridad de información. Es decir toda organización donde se tiene implementado infraestructura de redes es indispensable contar con políticas de seguridad que permitan proteger los activos considerados de valor.
- Usuarios que hacen uso de los recursos de la infraestructura de red.
- Usuarios Invitados

5.1.6 Responsabilidades y Cumplimiento

La Política de Seguridad aprobadas por el Gerente o Director debe ser de conocimiento obligatorio para todo el personal de la organización, independientemente de la situación de trabajo, el proceso a la cual esté anexada o el nivel de las tareas que desempeñe. Para llevar a efecto este trabajo se debe tener en cuenta las siguientes directivas de responsabilidad.

5.1.7 Declaración de Políticas de Seguridad

"Todo administrador de red sabe que debe estar preparado para el próximo ataque a sus sistemas y que es probable que sea desde su red interna. El administrador de red sabe que los usuarios internos son más peligrosos que los usuarios externos, dado que el 99% de los puertos de las redes LAN están desprotegidos." (Muñoz, 2011)

5.1.7.1 *Políticas tecnológicas para mitigar las Vulnerabilidades Ataques VLAN HOPPING*

5.1.7.1.1 *Políticas de Seguridad para evitar Ataque Switch Spoofing*

Mitigación: Sólo se puede explotar cuando se establecen interfaces para negociar un enlace trunk. Para evitar este ataque en switches Cisco, utilice las siguientes políticas de seguridad:

1. No usar VLAN nativa 1 en los puertos trunk. Colocar los puertos de acceso en modo access.

SW #conf t
SW (config)#interface FastEthernet0/1
SW (config-if)# switchport mode trunk
SW (config-if)# switchport trunk native vlan 2
SW (config-if)#end
SW (config)#exit

2. Crear una VLAN XY, poner a todos los puertos sin uso a la VLAN XY, declarar estos puertos sin uso en modo “Access”

SW(config) # configure terminal
SW(config-if) # show interfaces status
SW(config-if) # vlan 999
SW(config if-vlan) # name XY
SW(config if-vlan) # exit
SW(config-if) # int range g1/0 – 3
SW(config-if)# switchport mode access
SW (Config if-range) # sw mode acc vlan 999

3. Poner los puertos de acceso en modo “Access”

SW(config)# interface gigabitethernet 0/3
SW(config-if)# switchport mode access
SW(config-if)# exit

4. Deshabilitar DTP: Nunca dejar un puerto de acceso en modo "Dynamic Desirable ", "Auto Dynamic" o "Trunk".

SW (config)# interface gigabitethernet 0/3
SW (config-if)# switchport trunk encapsulation dot1q
SW (config-if)# switchport mode trunk
SW (config-if)# switch port nonegotiate

5. Apagar todos los puertos no utilizados con el comando shutdown y colocar los puertos de acceso en modo access.

SW (Config-if) # int range g1/0 – 3
SW(config-if)# switchport mode access
SW (Config if-range) # shutdown

5.1.7.1.2 *Políticas de Seguridad para evitar el Ataque Double Tagging*

Para la mitigación del Ataque Double Tagging se aplica la política 1, política 2 y política 3 de la mitigación del Ataque Switch Spoofing y agrega:

1. Etiquetado explícito de la VLAN nativa en todos los puertos trunk. Debe configurarse en todos los switches de la red.

SW (config) # vlan dot1q tag native

5.1.7.2 *Políticas para mitigar las Vulnerabilidades Organizacionales, Operacionales Y Físicas de los Ataques VLAN HOPPING*

Las políticas de seguridad son fáciles de entender tienen mucho que ver con el cumplimiento de controles y para ello hemos tomado como referencia la ISO 27002 y se ha relacionado con las vulnerabilidades operativas, organizaciones y físicas para contrarrestar los ataques Switch Spoofing y Double Tagging.

En esta sección del documento se presenta una propuesta de políticas de seguridad, con sus respectivos artículos, como un recurso para mitigar los Ataques VLAN HOPPING.

- Políticas de Seguridad de la Información
- Seguridad relativa a los recursos humanos:
- Control de acceso
- Seguridad física y del Entorno
- Seguridad de las comunicaciones
- Gestión de incidentes de seguridad de la información
- Cumplimiento

5.1.7.2.1 *Políticas de Seguridad de la Información (A.5)*

En toda organización la información es considerada el activo de valor más importante por lo tanto requiere ser protegida de amenazas internas, deliberadas o accidentales, generadas por los ataques VLAN HOPPING dentro de la red LAN. Las Políticas de Seguridad de la Información permitirán asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, así como también debe ser un compromiso de las Autoridades la difusión y cumplimiento por parte de todo el personal de la organización. Entre estas políticas tenemos:

Artículo 1°.- Es importante nombrar al responsable de cada activo o proceso de seguridad, aprobar y respaldar el documento por parte de la Dirección conjuntamente con Activos Fijos.

Artículo 2°.- Toda organización debe contar con una manual de políticas de seguridad o a actualizar si existe, tratando de mejorarla.

Artículo 3°.- El conocimiento de la política y su aplicación es fundamental pues una política pierde valor si no la conoce nadie.

Artículo 4°.- Las políticas deben ser conocidas y aceptadas por el personal de la organización con firma de responsabilidad.

Artículo 5°.- Cada uno de los empleados deben tener acceso al documento, incluso debe haber un documento resumen para los usuarios invitados.

Artículo 6°.- Establecer guía de buenas prácticas para usuarios según perfiles

5.1.7.2.2 *Seguridad relativa a los recursos humanos (A.7)*

Siendo el personal la principal amenaza dentro de la red LAN se debe tener consideración.

Artículo 1°.- **Antes de la contratación.**

- Investigación de antecedentes, es decir verificar hoja de vida, referencias personales que permitan determinar el perfil del empleado. Es decir explicar las responsabilidades referentes a políticas de seguridad en la etapa de reclutamiento de personal
- Términos y condiciones de contratación, se debe establecer claramente las responsabilidades y obligaciones que deben ser cumplidas y debe ser incluidas en el contrato a firmarse verificando su cumplimiento durante su período como empleado.

Artículo 2°.- **Durante la contratación.**

- Incorporación de la Seguridad en los puestos de trabajo, con la finalidad de controlar el uso incorrecto de las instalaciones y recursos, actos ilícitos, error humano y manejo no autorizado de la información las funciones y responsabilidades en materia de políticas de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.
- Control y Política del Personal, establecer las herramientas y mecanismos necesarios para realizar controles de verificación del personal.
- Compromiso de Confidencialidad para todo el personal y usuarios externos. La copia firmada del Compromiso deberá permanecer en el proceso de Talento Humano donde se listará las actividades que pueden ser objeto de control y

monitoreo, teniendo cuidado de no vulnerar el derecho a la privacidad del empleado.

Artículo 3°.- **Capacitación del Usuario**:

- Formación y Capacitación sobre Políticas de Seguridad, es imprescindible la capacitación de las políticas de seguridad a todo el personal de la organización así como también de los usuarios externos, se deberá planificar capacitaciones periódicas o cuando se amerite según sea el caso, tratando temas como uso correcto de los recursos informáticos, normas y procedimientos.
- La respuesta a Incidentes o anomalías en materia de seguridad, debe ser inmediata es decir trabajar como equipo de trabajo y comunicar de incidentes, debilidades relacionado con la seguridad informática en cuanto a hardware y software.

5.1.7.2.3 *Control de acceso (A.9)*

En toda organización se debe establecer requisitos para el control de accesos.

Artículo 1°.- **Política de control de accesos**

El control de acceso a las redes y servicios asociados, la asignación de perfiles de administrador, la administración de una red LAN es la responsabilidad del administrador es quien certificará que la red es segura, es el encargado de analizar y controlar quien puede tener acceso a la red según el permiso adecuado.

Artículo 2°.- **Responsabilidades del usuario.**

- Uso de información confidencial para autenticación según perfiles de usuario.
- Los cambios que se realicen en los equipos de la infraestructura de res deberán contar con su respectiva documentación, donde se describe los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

Artículo 3°.- **Control de acceso a sistemas y aplicaciones.**

En toda organización, debe existir un Coordinador del Comité de Seguridad adscrita al Comité de Seguridad. Esta coordinación es responsable de implementar las políticas de

seguridad en informática y de comunicaciones, así como velar por el cumplimiento de dichas normas en la red interna de la organización.

- Monitorear las tecnologías de seguridad es responsabilidad del o los administradores de red, trabajo que se realiza con el apoyo de los técnicos de quienes conforman el Departamento de Tecnologías y Comunicaciones.
- La aplicación de los mecanismos de autenticación y permisos de acceso a la red, deben ser aprobados por el Departamento de Tecnologías y Comunicaciones
- Definir el control de acceso a los dispositivos para prevenir usos inadecuados por parte de usuarios no autorizados.
- Ejecutar una gestión centralizada de los dispositivos.
- Cifrar los datos sensibles asegurando la confidencialidad.
- Gestionar un control de políticas de puntos de acceso.
- Prevenir las fugas de información.

Artículo 4°.- **Identificadores de usuario y contraseñas**

- El personal y los usuarios terceros dispondrán de autorización con usuario y contraseña.
- Para tener un identificador de acceso a la Red de Comunicaciones, recursos informáticos debe aceptar formalmente la política de seguridad vigente.
- Según los perfiles de usuario se obtendrá acceso autorizado a datos y recursos, establecidos por el responsable de la información.
- Las contraseñas debe ser fuertes es decir de ocho caracteres o más que contengan letras mayúsculas, minúsculas, números y símbolos alfanuméricos.
- Los usuarios temporales tendrán acceso por un periodo de tiempo determinado una vez expirado, se desactivarán del sistema.

Artículo 5°.- **Software**

- El personal y usuarios terceros no puede instalar programas sin autorización, se trabaja con cuentas de usuarios.
- El personal y usuarios terceros tienen prohibido borrar programas instalados legalmente, configurado con cuentas de administrador.

Artículo 6°.- **Recursos de red**

El personal de la organización y los usuarios terceros no debe:

- Conectar ningún tipo de equipo de comunicaciones sin previa autorización.
- Obtener derechos o accesos diferentes a aquellos que les hayan sido asignados según las políticas de seguridad socializadas.
- Intentar falsear los registros "log" de los Sistemas de Información.
- Intentar descifrar las claves de los sistemas, cuentas de usuario, o equipos de seguridad.
- Ejecutar hacking ético que provoque daños a los recursos Informáticos o sistemas de información.

Artículo 7°.- **Comité de Seguridad**

- Vigilar el funcionamiento de la infraestructura tecnológica en las diferentes áreas de la organización.
- Establecer planes de contingencias para respaldar información a corto, mediano y largo plazo
- Mantener actualizado el Inventario de los recursos informáticos conjuntamente con el proceso de Activos Fijos.
- Velar por el cumplimiento de las políticas y procedimientos establecidos.

5.1.7.2.4 *Políticas de Seguridad física y del Entorno (A.11)*

Esta Política es aplicable a todos los recursos físicos: Instalaciones, Equipamiento, Cableado e Información:

Artículo 1°.-Notificar e impedir accesos no autorizados a los equipos de comunicaciones y servicios de la organización.

Artículo 2°.-Salvaguardar la infraestructura de red en áreas protegidas

Artículo 3°.-Definir perímetro de seguridad, aplicando controles de acceso y medidas de seguridad adecuados.

Artículo 4°.-Resguardar el traslado del equipo cuando salga del área protegida a mantenimiento.

Artículo 5°.-Vigilar los factores ambientales que puedan perjudicar el correcto funcionamiento del equipamiento informático donde reside la información de la organización.

Artículo 7°.-El Comité de Seguridad definirá:

- Medidas de seguridad física y ambiental para proteger los activos
- Verificar el cumplimiento de las disposiciones sobre seguridad física y ambiental.

Artículo 8°.-El Responsable del Área Informática controlará

- Mantenimiento del equipamiento informático basado en las indicaciones del proveedor dentro y fuera de las instalaciones de la Organización.

Artículo 9°.- Los Responsables de Unidades Organizativas

- Definen los niveles de acceso físico del personal a las áreas seguras bajo su responsabilidad.

Artículo 10°.-Los Propietarios de la Información

- Autorizarán formalmente mediante quipux o correo institucional el trabajo fuera de las instalaciones

Artículo 11°.-Perímetro de Seguridad Física

- Creación de medidas de control físicas alrededor de las instalaciones de procesamiento de información.
- El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. (Laporte, 2016)

Artículo 12°.- Controles de Acceso Físico

- Permitir el acceso a las áreas protegidas sólo al personal autorizado mediante el empleo de controles.
- Asegurar tareas del personal y de usuarios terceros en las áreas protegidas mediante controles y lineamientos adicionales.
- Sólo al personal autorizado tiene acceso la información confidencial.
- El usuario externo puede ingresar a las instalaciones consideradas áreas seguras únicamente bajo la vigilancia de personal autorizado.

Artículo 13°.- Ubicación y protección del equipamiento y copias de seguridad

- Para reducir las amenazas de acceso no autorizado el equipamiento será ubicado en un área protegida.

Artículo 14°.- Suministros de Energía

- El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía otras anomalías eléctricas. (Laporte, 2016)

Artículo 15°.- Seguridad del Cableado

- Proteger el cableado de energía y de telecomunicaciones realizando conexiones adecuadas. (Laporte, 2016)
- Los cables deben estar aislados y debidamente etiquetados para cuando suceda algún problema, pueda solucionarlos de manera fácil.
- Proteger el cableado de red contra Intercepción no Autorizada,
- El cableado debe ser transportado a través de canaletas para su adecuada protección.
- Los cables deben estar etiquetados de forma clara para facilitar la identificación de los elementos conectados y evitar desconexiones erróneas.
- Cada organización debe contar con planos que describan las conexiones del cableado.
- El acceso a los centros de cableado (Racks), debe estar protegido

Artículo 16°.- Mantenimiento de Equipos

- Monitorear equipos de comunicaciones, equipos de seguridad.
- Para los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, se debe trabajar conjuntamente con el personal especialista y debidamente autorizado e identificado de Mantenimiento
- Registrar las fallas del mantenimiento preventivo o correctivo realizado a los servidores, switches, routers, equipos de comunicaciones, equipos de seguridad.

Artículo 17°.- Retiro de los Bienes

- Para el retiro del equipamiento, la información y el software debe ser con autorización formal

Artículo 18°.- Controles físicos de entrada.

- El Departamento de Tecnologías de Información y Comunicaciones es el responsable del acceso físico a los equipos y de la administración física de los servidores, pcs, router, switches.

Artículo 19°.- Instalaciones de equipos

Para instalar un equipo, se deberá seguir los siguientes lineamientos:

- Los equipos como servidores, switch, router se instalará en áreas seguras, alejado del tráfico de personas.
- El Departamento de Tecnologías de la Información y Comunicaciones deberá contar con mapas actualizado de las instalaciones eléctricas y de comunicaciones de la infraestructura de red.
- Las instalaciones eléctricas y de comunicaciones deben estar fijas mediante canaletas y fuera del alcance de personas o máquinas, protegidos de la interferencia eléctrica o magnética.
- Las instalaciones irán de acuerdo a los requerimientos de los equipos, cumpliendo las especificaciones de cableado estructurado
- Planificar adecuadamente evitando instalaciones improvisadas o sobrecargadas.

Artículo 20°.- Seguridad de los equipos.

- Asegurar todos los dispositivos en áreas seguras que este separado del acceso no autorizado.
- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

5.1.7.2.5 *Seguridad de las comunicaciones (A.13)*

Artículo 21°.- Del cuarto de comunicaciones

- El cuarto de comunicaciones es el principal componente en una organización, el acceso debe ser restringido y solamente autorizado por el Jefe de Redes y Comunicaciones.
- Los equipos de servicios de red, deben encontrarse alojados en el cuarto de comunicaciones.

- El cuarto de comunicaciones deben poseer aire acondicionado y un sistema de ventilación de acorde a las dimensiones del mismo.

5.1.7.2.6 *Gestión de incidentes de seguridad de la información (A.16)*

Artículo 1°.- Respuesta a incidentes y anomalías de seguridad

- Los respaldos de información de los procesos se realizarán trimestralmente según la planificación o dependiendo de la información y deberá ser almacenados en un dispositivo seguro protegido de robos.
- Los respaldos se utilizarán únicamente en casos especiales, debido a su importancia.
- Las organizaciones realizar respaldos de información de los servidores ante cualquier incidente.

5.1.7.2.7 *Cumplimiento (A.18)*

- El personal de la organización debe entender los objetivos de la administración y la responsabilidad que representa en relación al cumplimiento de las políticas de seguridad; pero también debe ser consciente de las consecuencias del no cumplimiento.
- El orden disciplinario tendrán que estar enmarcadas según la normativa legal vigente de la organización respetando además los derechos fundamentales de los trabajadores y la legislación laboral vigente previamente aprobada y socializada por el Comité de Seguridad.
- Las organizaciones deben considerar obtener la confirmación escrita de usuarios finales y empleados diciendo que han leído, comprendido y aceptado las políticas de seguridad de información de la organización.

5.1.8 Vigencia de las Políticas

Las Políticas descritas en el documento entrarán en vigencia, desde su aprobación por la máxima autoridad de la organización y serán mejoradas por el Departamento de Tecnologías de la Información y Comunicaciones, de acuerdo a los cambios en la infraestructura y servicios de tecnologías de la Organización.

CONCLUSIONES

Las vulnerabilidades de los ataques VLAN HOPPING son el resultado de las configuraciones débiles de los puertos del switch y de la ausencia de políticas de seguridad en redes LAN donde el principal enemigo es el usuario interno por las prioridades y permisos que tiene dentro de la organización, lo que facilita el acceso no autorizado a información que en la mayoría de casos es de carácter confidencial.

Para el levantamiento de las políticas de seguridad se revisó la ISO 27002 aquellas que estaban relacionadas con el tema de investigación, básicamente relacionadas con las vulnerabilidades organizacionales, operacionales y físicas, las que una vez aplicadas se observó que si se mitigan los ataques VLAN HOPPING con sus dos técnicas Switch Spoofing y Double Tagging e identificar las vulnerabilidades.

Al implementar el ambiente de prueba, se presentaron inconvenientes con las imágenes de switch, las versiones c2691, c3640, c3725, c7200 no soporta el comando switchport nonegotiate, que evita que el puerto permanezca en modo troncal, por lo que se utilizó las imágenes IOU Cisco L2 y L3 y al aplicar las políticas de seguridad las vulnerabilidades de ataques VLAN HOPPING a nivel de la Capa de Enlace de Datos en redes LAN se mitigaron hasta llegar al 0%.

Al aplicar las políticas de seguridad basados en la Norma ISO 27002 se consiguió determinar las vulnerabilidades operativas, organizacionales y físicas que existen en la red de área local LAN que ponen en peligro la protección de los elementos físicos de la organización en cuanto a los Ataques VLAN HOPPING, entre estás tenemos políticas de seguridad de la Información, seguridad relativa a los recursos humanos, control de acceso, seguridad física y del entorno, seguridad de las comunicaciones, gestión de incidentes de seguridad de la información y cumplimiento

RECOMENDACIONES

Toda organización tanto pública y privada esta propende a ataques informáticos, por lo que es recomendable la implementación de políticas de seguridad a nivel de LAN por seguir siendo el área más vulnerable de las organizaciones, debido a que los usuarios internos son quienes tienen mayor privilegio y permisos para poder acceder a información confidencial, es decir ingresar a cualquier lugar de la organización sin ninguna restricción.

A pesar de la identificación de las vulnerabilidades, es recomendable que las organizaciones estén preparadas para superar cualquier eventualidad que dificulte las actividades diarias del personal, esto se logra el Departamento de Tecnologías de la Información y Comunicaciones debe regular el cumplimiento y evaluación en cuanto a la aplicación de las políticas de seguridad.

Se recomienda a toda organización realizar una tabla de mapeado controles NIST en controles ISO 27002 y determinación de métricas, con el propósito de verificar y reforzar la efectividad de los controles implementados, aplicando incluso la metodología GQM (Métricas de Metas por Cuestionario), que significa establecer metas para luego plantear preguntas cuyas respuestas las métricas, permitirán tener un visión más clara sobre el estados de la infraestructura de red.

Como trabajo futuro, se podría ampliar el objeto de estudio y realizar ataques combinados utilizar virtualización para levantar escenarios más cercanos a la realidad y ejecutar los ataques VLAN HOPPING y a partir de ellos probar otros ataques como ARP Spoofing; incluso se podría realizar las pruebas con switches que no sean marca CISCO.

BIBLIOGRAFÍA

Á**lvarez, W**. (2014). *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

Andrés, A., & Barroso, D. (2009). *S21sec blog. Seguridad Digital.: ataques sobre el nivel 2 del modelo osi (vii): 802.1q*. Recuperado 17 de mayo de 2015, a partir de http://blog.s21sec.com/2009/06/ataques-sobre-el-nivel-2-del-modelo-osi_25.html

Avalos, I. (2012). *Carrera de Telecomunicaciones: Cap. VII Capa Enlace De Datos.* Recuperado 6 de mayo de 2017, a partir de http://fdbk-teleco.blogspot.com/2012/09/cap-vii-capa-enlace-de-datos.html

Baxevanos, I. (2014). *Protecting with network security strategies a medium size enterprise and implementing scenarios attacks and countermeasures on cisco equipment. university of piraeus*. Recuperado a partir de http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/6443/mte1118.pdf?sequence=1&isallowed=y

Bull, R. (2014). *A critical analysis of layer 2 network security in virtualized environments.* Recuperado a partir de http://people.clarkson.edu/~bullrl/classes/dissertation/proposal/bullrl_proposal.pdf

Bull, R. (2015). *Vlan Security*. Recuperado a partir de http://people.clarkson.edu/~bullrl/classes/cs708/bullrl_cs708_s15.pdf

Bull, R., & Matthews, J. (2013). *Exploring layer 2 network security issues in virtualized environments*. Recuperado a partir de http://people.clarkson.edu/~bullrl/classes/cs657/bullrl_cs657_project.pdf

Bull, R., Matthews, J., & Trumbull, k. (2016). *Vlan hopping, Arp Poisoning & man-in-the-middle attacks in virtualized environments*. Recuperado a partir de https://ronnybull.com/assets/docs/bullrl_defcon24_slides.pdf

Capella, J. (2012). *Características y configuración básica de VLANS.* Recuperado a partir de https://riunet.upv.es/handle/10251/16310

Collazos, M. (2013). *La nueva versión 27000:2013 . Un cambio en la integración de los sistemas de gestión.* Recuperado 9 de marzo de 2017, a partir de file:///c:/users/nopia/downloads/presentacion_manuel_collazos_-_1.pdf

De Nova, J. (2012). *Tutorial Gns3.* Recuperado a partir de https://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf

Deivid. S. (2016). *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

Díaz, A. (2014). *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/

Gaddis, J. (2011). *Free CCNA Labs – Cisco Ios-On-Unix (iou) — Free Ccna Labs*. Recuperado 19 de abril de 2017, a partir de http://freeccnalabs.com/cisco-iou/

Ges, C. (2013). *Controles ISO 27002-2013*. Recuperado 9 de marzo de 2017, a partir de http://www.iso27000.es/download/controlesiso27002-2013.pdf

Herón, S. (2013). *Ten top threats to vlan security - redscan.* Recuperado 24 de noviembre de 2016, a partir de https://www.redscan.com/news/ten-top-threats-to-vlan-security/

Herrera, F. (2015). *Explicando el VLAN hopping*. Recuperado 2 de mayo de 2015, a partir de https://es.scribd.com/doc/58116973/10/explicando-el-vlan-hopping
herzog, p. (2003). osstmm.2.1.es - manual de la metodología abierta de testeo de seguridad - osstmm.es.2.1.pdf. recuperado 19 de mayo de 2017, a partir de https://radiosyculturalibre.com.ar/biblioteca/infosec/osstmm.es.2.1.pdf

Laporte, J. (2016). *Manual de seguridad de la información | Buenos Aires ciudad - gobierno de la ciudad autónoma de Buenos Aires.* Recuperado 18 de abril de 2017, a partir de http://www.buenosaires.gob.ar/sindicatura/manual-de-seguridad-de-la-informacion

López, A., & Ruiz, X. (2012). *ISO27000.es - El portal de iso 27001 en español. Gestión de seguridad de la información*. Recuperado 8 de marzo de 2017, a partir de http://www.iso27000.es/

Maguana, A. (2015). *Protocolos de la capa de enlace de datos: trama | telecomunicaciones.* Recuperado 21 de abril de 2017, a partir de http://alexandramaguanatelecomunicaciones.blogspot.com/2014/07/protocolos-de-la-capa-de-enlace-de.html

Mejía, C., Ramírez, N., & Rivera, J. (2012). *Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo osi en las redes de datos de las*

organizaciones. Universidad tecnológica de Pereira, Colombia. Recuperado a partir de http://repositorio.utp.edu.co/dspace/bitstream/11059/2734/1/0058r173.pdf

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

Muñoz, A. (2011). *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

Ochoa, V. (2011). *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*. (Tesis de pre o posgrado, Escuela Superior Politécnica del Ejercito). Recuperado a partir de http://repositorio.espe.edu.ec/bitstream/21000/4984/1/t-espe-032019.pdf

Pascal, L., & Petre, D. (2005). *Networking - ICN 2005: 4th International Conference on Networking. Springer Science & Business Media.* Recuperado a partir de https://books.google.com.ec/books?id=geqdcaaaqbaj&dq=vlan+hopping+attacks

Patiño, L. (2014). *Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, propolsinecor. Universidad Nacional Abierta y a distancia "UNAD"*. Recuperado a partir de http://repository.unad.edu.co/bitstream/10596/2742/1/12973210.pdf

Revista, G. (2015). *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

Rouiller, S. (2006). *Virtual Lan Security: weaknesses and countermeasures*. Recuperado 11 de diciembre de 2016, a partir de http://u.askapache.com/2006/12/vlan-security-3.pdf

Sangoluisa, D. (2015). Definición de las políticas de seguridad de la información para la red convergente de la presidencia de la república del ecuador basado en las normas iso 27000. Escuela Politécnica Nacional. Recuperado a partir de http://bibdigital.epn.edu.ec/bitstream/15000/11462/1/cd-6488.pdf

Santos, I. (2011). *Capas del modelo OSI - sistemas de multiplexado.* Recuperado 6 de mayo de 2017, a partir de https://sites.google.com/site/sistemasdemultiplexado/arquitecturas-de-las-redes-de--comunicacin-caractersticas/3--el-modelo-osi-o-de-capas/capas-del-modelo-osi

Siddique, N., Ali, M, & Zubair, M. (2015). Data Link Layer Security problems and solutions. Recuperado a partir de http://www.diva-portal.org/smash/get/diva2:783188/fulltext01.pdf

Tejada, M. (2013). *Fundamento de las telecomunicaciones: Capa de Enlace de Datos.* Recuperado 26 de febrero de 2017, a partir de http://actividad-telematica.blogspot.com/2013/05/capa-de-enlace-de-datos.html

Velandia, R. (2012). *Protocolo DTP*. Recuperado 8 de mayo de 2017, a partir de http://networksgoldencross.blogspot.com/2012/06/protocolo-dtp.html

Wares, M. (2011). *Top 15 de herramientas y utilidades de seguridad/hacking*. Recuperado 19 de abril de 2017, a partir de http://mikewarez.blogspot.com/2011/07/top-15-de-herramientas-y-utilidades-de.html#.wpchn6k1tpz

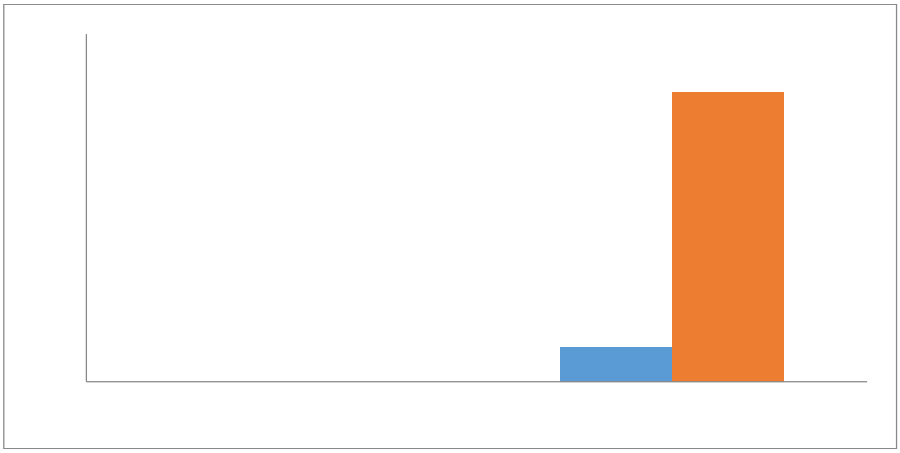
ANEXOS

Anexo A: Encuesta que justifica el desarrollo del tema de tesis

Objetivo: Determinar el grado de conocimiento del personal del Departamento de Información y Comunicaciones acerca de los ataques de Capa 2, ataques VLAN HOPPING; técnicas de protección

1. **Dentro de su organización conoce que tipo de DTP está habilitado en los swich Cisco por defecto?**

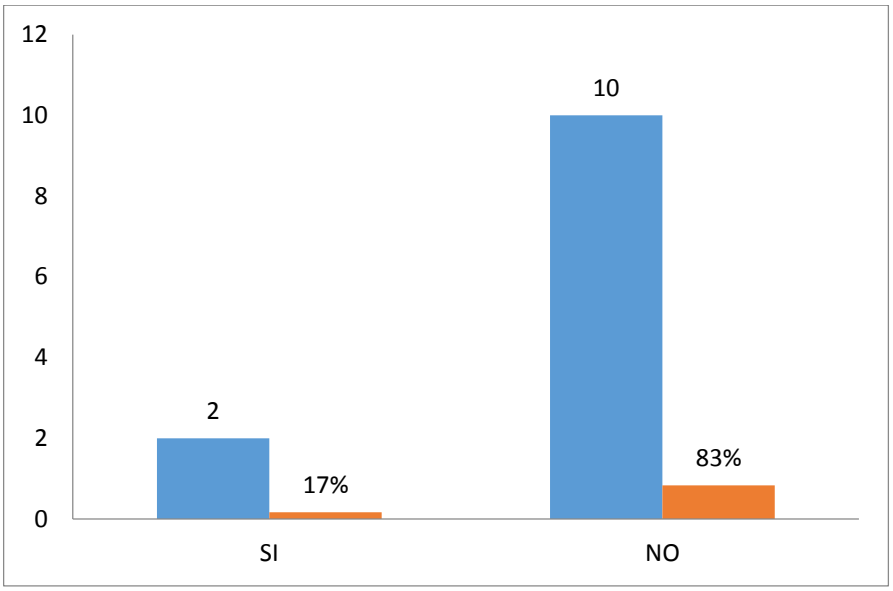
SI	NO
0	12
0%	100%



El DTP se habilita automáticamente en un puerto del switch cuando se configura un modo de trunking adecuado en dicho puerto. Para ello el administrador debe ejecutar el comando switchport mode adecuado al configurar el puerto: switchport mode {access | trunk | dynamic auto | dynamic desirable}. Con el comando switchport nonegotiate se desactiva DTP. Su función es gestionar de forma dinámica la configuración del enlace troncal al conectar dos switches, introduciendo los comandos del IOS (sistema operativo de los switches y routers Cisco) en la configuración del dispositivo (running-config) de forma automática sin que el administrador intervenga. Según los datos obtenidos se puede observar que el 100% de los entrevistados manifiestan que desconocer acerca del tema.

2. **Dentro de la organización el uso de la VLAN NATIVA es frecuente?**

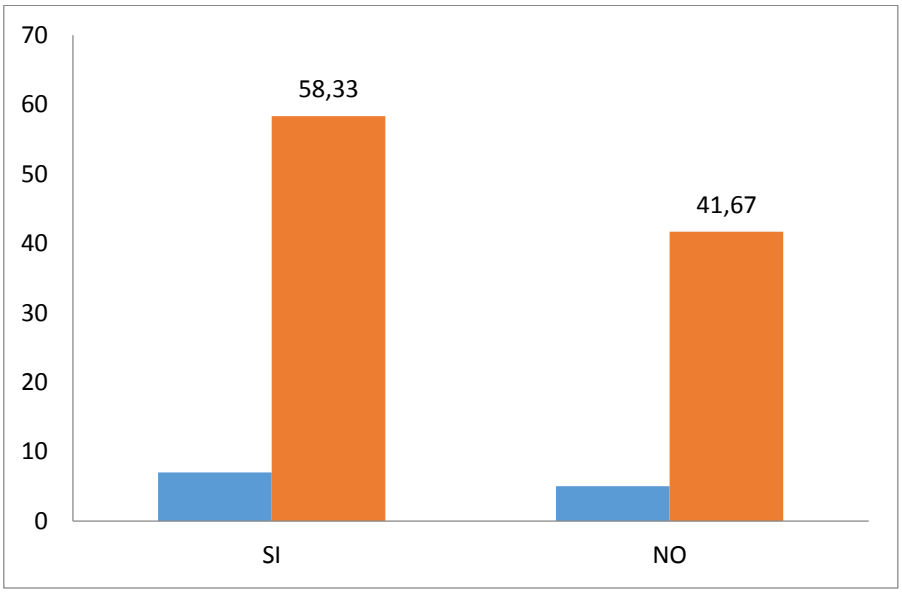
SI	NO
2	10
17%	83%



La **VLAN nativa** es una condición usada con interfaces que son configuración como**vlan** troncales (enlaces troncales). Las tramas de todas las **vlan** son trasportadas por un enlace en modo troncal, por medio de la un tag que puede ser 802.1Q o ISL, exceptuando a esto, las tramas que pertenecen a la **vlan** . Según los datos obtenidos el 17% del personal entrevistado afirma que el uso de la VLAN NATIVA es frecuente, mientras que el 83% confirma que no.

3. En cuanto a la configuración de los puertos de acceso como en modo Access?

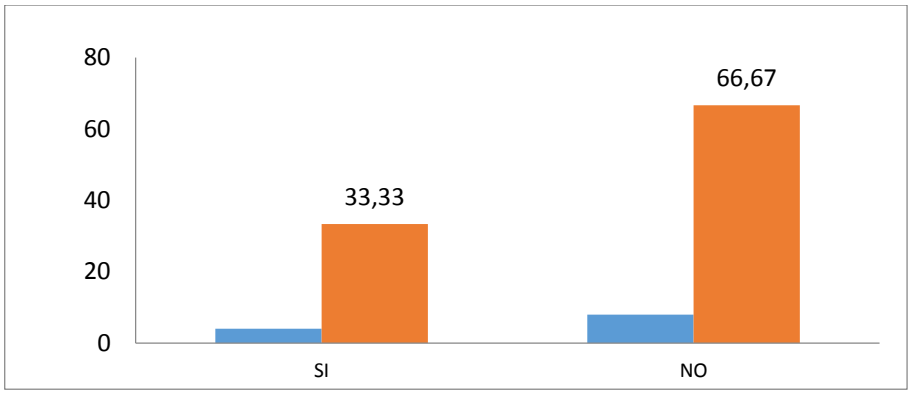
SI	NO
7	5
58%	42%



Access: La principal utilidad que se les da a este tipo de puertos es para conectar equipos finales, los puertos de acceso solo transportan tráfico de una sola vlan y aunque los puertos de acceso también se pueden utilizar para conectar switches no es recomendable ya que una implementación de este tipo no es escalable. El 58,33% del personal considera que existen permisos para acceder a información confidencial, mientras que el 41.67 % manifiesta que no.

4. Conoce el número de puertos sin uso habilitados?

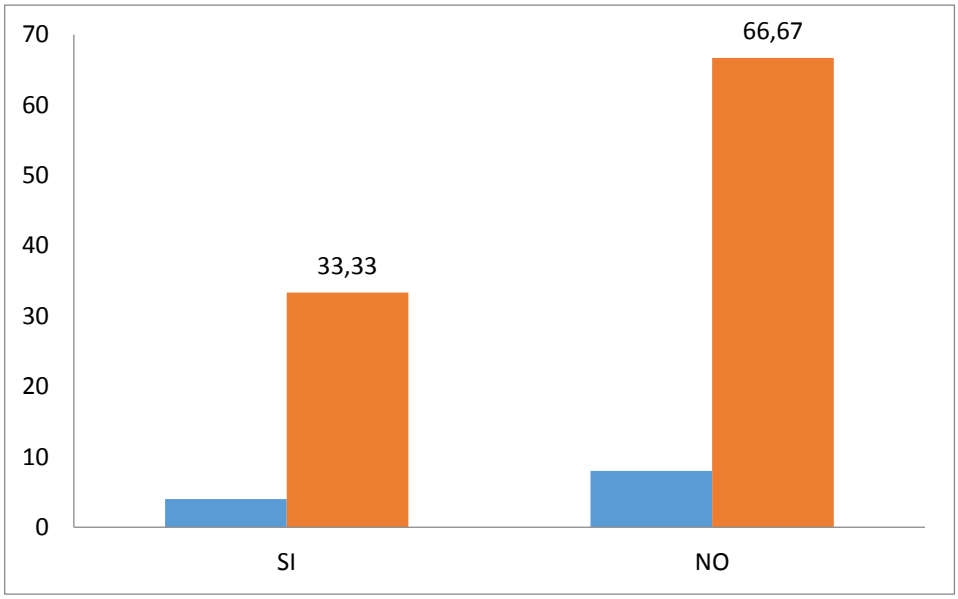
SI	NO
4	8
33,33	66,67



Un puerto de computadora sirve como interfaz para enviar y recibir datos entre el computador y otros computadores o dispositivos periféricos. Un puerto de computadora es una ranura o toma de corriente de un equipo en el cual se enchufa un conector que regularmente contiene un cable. Los puertos que permiten conectar dispositivos, generalmente se encuentran en la parte posterior, frontal o lateral de un equipo, el 33.33% considera que la aplicación de políticas de seguridad no permite el acceso no autorizado a la red, mientras que el 66.67% consideran que no.

5. Dentro de su organización existe seguridad de la Información?

SI	NO
4	8
33,33	66,67



La **seguridad de la información** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la **información** buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma. Según los datos obtenidos se puede determinar que el 66.67% de los administradores manifiestan, mientras que el 33.33% si lo realizan.

Anexo B ISO 27002

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATRONICADO POR:

GES|CONSULTOR

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Anexo C: Configuraciones del Escenario de Pruebas

Switch 1:

Tiene creadas las Vlan 10, 20 y 30 y asignados los puertos correspondientes a cada VLAN, como se muestra en la Gráfico 3-1.

SW1

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/3, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3, Et3/0, Et3/1, Et3/2
                                                Et3/3
10   VLAN0010                         active    Et0/1
20   VLAN0020                         active    Et0/2
30   VLAN0030                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
```

Gráfico 3-1: **Creación VLAN 10, 20 y 30**

Elaborado por: **Pilamunga Norma, 2017**

En el Gráfico 3-2 se muestra el puerto Et0/0 está configurado en modo trunk, como se muestra

```
IOU1#sh interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10,20,30
IOU1#
```

Gráfico 3-2: **Configuración en modo trunk**

Elaborado por: **Pilamunga Norma, 2017**

Switch 2:

Prácticamente son las mismas configuraciones que el switch 1 (Gráfico 3-3)

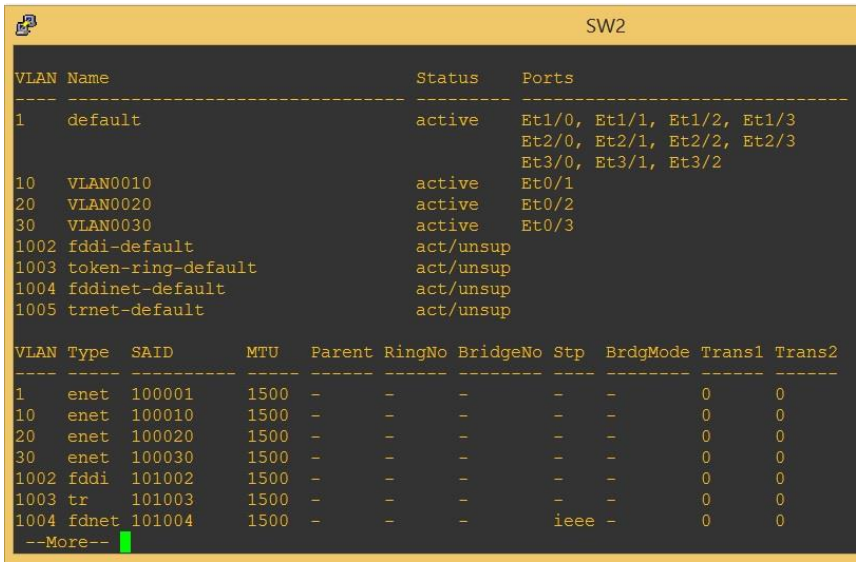


Gráfico 3-4: **Creación VLAN Switch 2**

Elaborado por: **Pilamunga Norma, 2017**

Tiene configurados los puertos Et0/0 y Et3/3 en modo trunk Gráfico 3-6 ya que el uno va conectado al Swtich 1 y el otro al Router.

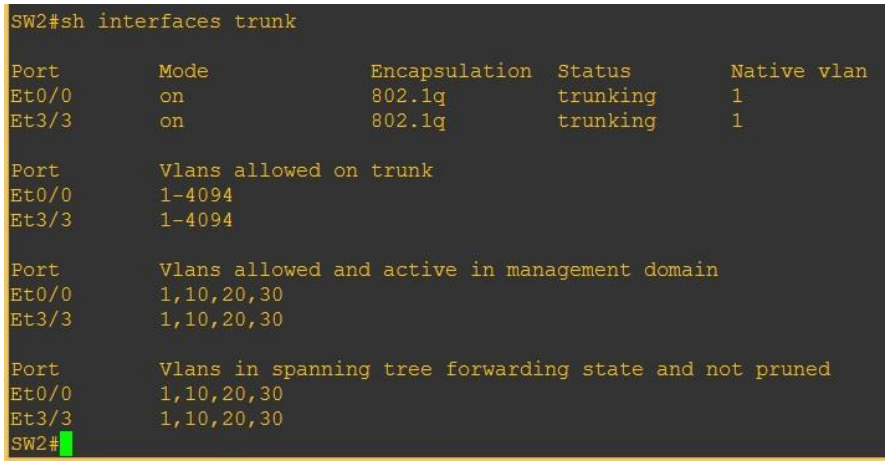


Gráfico 3-5: **Configuración de los puertos Et0/0 y Et3/3 en modo trunk**

Elaborado por: **Pilamunga Norma, 2017**

Configuración Router:

VLAN Routing, Gráfico 3-6.

```
R1#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/0.10         192.168.10.1    YES NVRAM  up                    up
FastEthernet0/0.20         192.168.20.1    YES NVRAM  up                    up
FastEthernet0/0.30         192.168.30.1    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet2/0         unassigned      YES NVRAM  administratively down down
Serial3/0                  unassigned      YES NVRAM  administratively down down
Serial3/1                  unassigned      YES NVRAM  administratively down down
Serial3/2                  unassigned      YES NVRAM  administratively down down
Serial3/3                  unassigned      YES NVRAM  administratively down down
```

Gráfico 3-6: **Configuración Router**

Elaborado por: **Pilamunga Norma, 2017**

VPCs:

PC2 – VLAN 20

Se encuentra en la Vlan20 y tampoco tiene puerta de enlace. Gráfico 3-7

PC2-Vlan20

```
VPCS> sh

NAME   IP/MASK              GATEWAY          MAC               LPORT  RHOST:PORT
VPCS1  192.168.20.11/24     0.0.0.0          00:50:79:66:68:01 10003  192.168.10.129:10002
       fe80::250:79ff:fe66:6801/64
```

Gráfico 3-7: **PC2 – VLAN 20**

Elaborado por: **Pilamunga Norma, 2017**

PC1 - VLAN 10

Se encuentra en la Vlan10 y no tiene puerta de enlace. Gráfico 3-8

PC1-Vlan10

```
VPCS> show

NAME   IP/MASK              GATEWAY          MAC               LPORT  RHOST:PORT
VPCS1  192.168.10.11/24     0.0.0.0          00:50:79:66:68:02 10010  192.168.10.129:10009
       fe80::250:79ff:fe66:6802/64
```

Gráfico 3-8: **PC1 - VLAN 10**

Elaborado por: **Pilamunga Norma, 2017**

Centos – VLAN 20

Se encuentra en la VLAN 20 y no tiene puerta de enlace. Gráfico 3-9

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:3E:3B:EF
          inet addr:192.168.20.129  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3e:3bef/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2835 (2.7 KiB)  TX bytes:2538 (2.4 KiB)
          Interrupt:19 Base address:0x2000
```

Gráfico 3-9: **Centos – VLAN 20**

Elaborado por: **Pilamunga Norma, 2017**

PC5 - VLAN 30

Se encuentra en la VLAN 30 y no tiene puerta de enlace. Gráfico 3-10

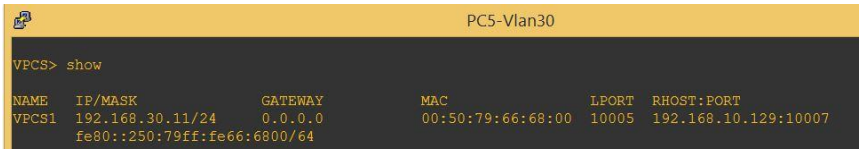


Gráfico 3-10: **PC5 – VLAN 30**

Elaborado por: **Pilamunga Norma, 2017**

Anexo D: Política 1 No usar VLAN nativa 1 en los puertos trunk. Colocar los puertos de acceso en modo access.

SW1

```
IOU1(config)#int e0/0
IOU1(config-if)#sw
IOU1(config-if)#switchport trunk nativ
IOU1(config-if)#switchport trunk native vl
IOU1(config-if)#switchport trunk native vlan 99
IOU1(config-if)#
```

Grafico 1 Política 1

Elaborado por: Pilamunga Norma, 2017

SW2

```
IOU2(config)#int e0/0
IOU2(config-if)#switchport trunk native vlan 99
IOU2(config-if)#
```

Grafico 2 Política 1

Elaborado por: Pilamunga Norma, 2017

```
IOU1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#int range e1/0 -3
IOU1(config-if-range)#sw
IOU1(config-if-range)#switchport mode
IOU1(config-if-range)#switchport mode acc
IOU1(config-if-range)#switchport mode access
IOU1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#int range e1/0 -3
IOU1(config-if-range)#sw
IOU1(config-if-range)#switchport mode
IOU1(config-if-range)#switchport mode acc
IOU1(config-if-range)#switchport mode access
IOU1(config-if-range)#sw
IOU1(config-if-range)#switchport no
IOU1(config-if-range)#switchport nonegotiate
IOU1(config-if-range)#sh
IOU1(config-if-range)#
```

Grafico 3 Política 1

Elaborado por: Pilamunga Norma, 2017

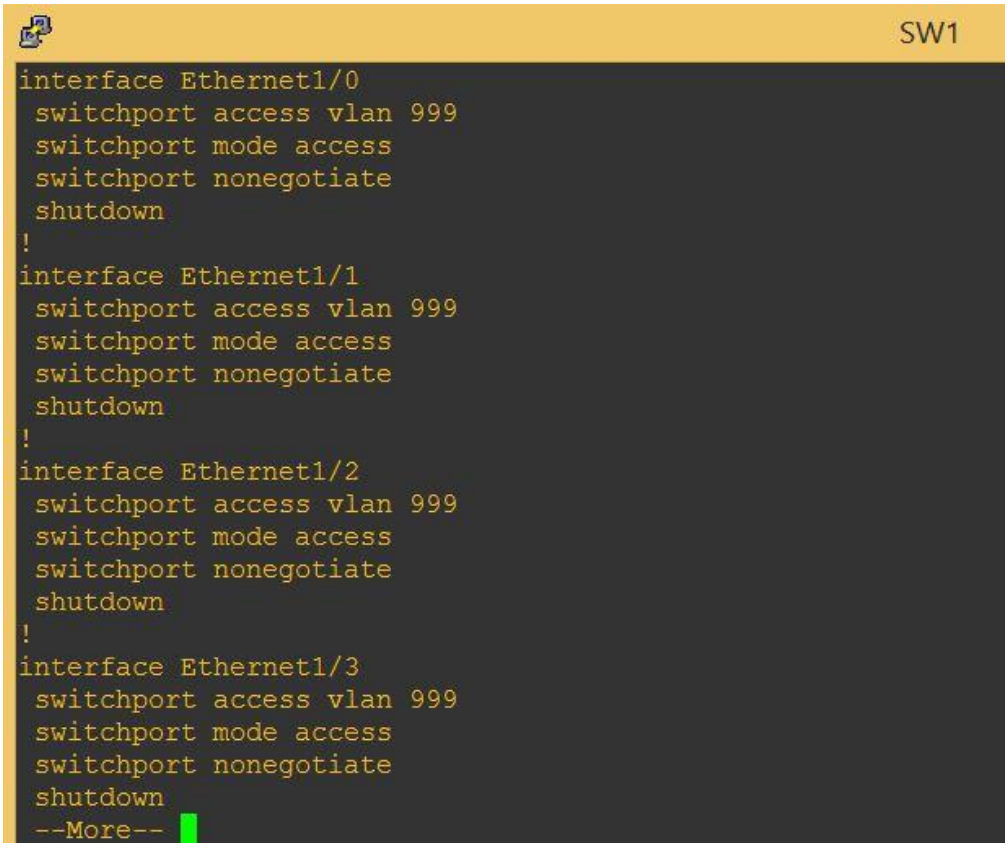


Grafico 4 Política 1

Elaborado por: Pilamunga Norma, 2017

```
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
```

Grafico 5 Política 1: No usar VLAN nativa 1. Colocar los puertos de acceso en modo access.

Elaborado por: Pilamunga Norma, 2017

Anexo E Política 2 Crear una VLAN XY, poner a todos los puertos sin uso a la VLAN XY y declarar estos puertos sin uso en modo "Access"

En el Gráfico1, 2 y 3 se observa los comandos ejecutados.

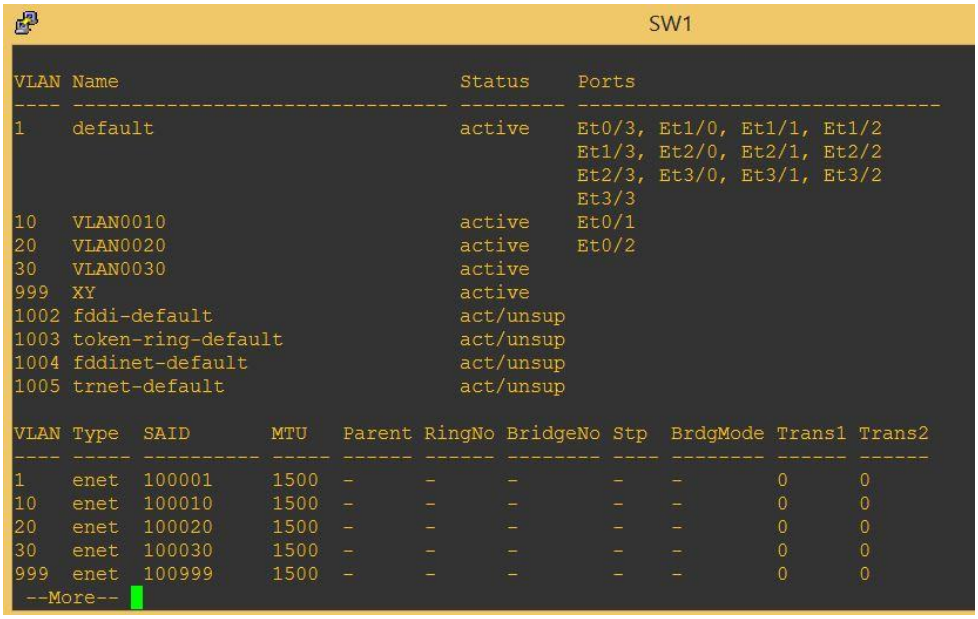


Grafico 1 Política 2

Elaborado por: Pilamunga Norma, 2017

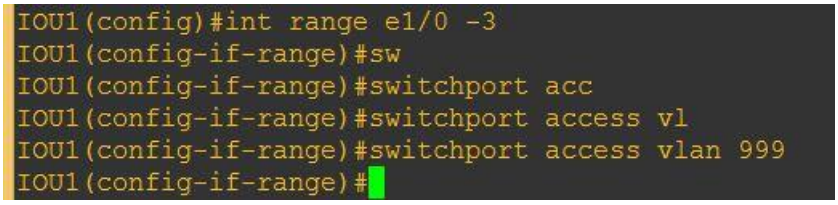


Grafico 2 Política 2

Elaborado por: Pilamunga Norma, 2017

Grafico 3 Política 2

Elaborado por: Pilamunga Norma, 2017

Anexo F Política 4 Deshabilitar DTP

Comenzamos configurar los puertos como modo access

```
IOU1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#int e0/1
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport nonegotiate
IOU1(config-if)#
```

Grafico 1 Política 4

Elaborado por: Pilamunga Norma, 2017

SW1

```
Name: Et0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

Grafico 2 Política 4

Elaborado por: Pilamunga Norma, 2017