ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN ESQUEMA PARA LA SEGURIDAD A NIVEL DE CAPA 2 EN LOS DISPOSITIVOS DE CONMUTACIÓN EN LA RED DE ÁREA LOCAL DE UNA EMPRESA"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

GUSTAVO JAVIER MAZZINI ALMEIDA

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A mi Dios por llenarme de vida y permitirme terminar con esta etapa profesional. A mi familia por el apoyo brindado. A mis padres por ser ejemplo a seguir con su constancia y a todos aquellos amigos y docentes que hicieron posible poder culminar con este reto profesional.

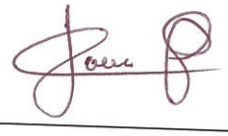
DEDICATORIA

El presente proyecto lo dedico a mis hijos por darme su compresión y tiempo durante el transcurso de esta maestría. A Sonia por la tenacidad de lucha y ejemplo de vida.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire C.

DIRECTOR DEL MSIA



Ing. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

Mgs. Karina Astudillo.

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

CIB - ESPOL

RESUMEN

El presente documento da a conocer un esquema para fortalecer las características en los dispositivos conmutadores de una red LAN luego de evidenciarse mediante el análisis las deficiencias en las configuraciones que pueden ser aprovechadas por un atacante y vulnerar la seguridad de la información, por lo cual se diseña un esquema, se lo implementa y se lo válida evidenciando de esa manera que se ha minimizado el riesgo de ser vulnerados ante un ataque a la infraestructura tecnológica.

Dentro del primer capítulo se describe el problema que hizo posible este trabajo mostrando la realidad encontrada en la infraestructura tecnológica de las redes corporativas en las empresas.

Continuando con el segundo capítulo se realiza el análisis de las configuraciones y vulnerabilidad de los protocolos STP, VTP, diseño del esquema y la implementación del mismo en los conmutadores CISCO que participan en este trabajo.

Y finalmente en el tercer capítulo se interpreta los resultados y se válida la aplicación del esquema propuesto y el cumplimiento del alcance descrito en la solución del problema planteado en este trabajo.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BPDU	Del inglés Bridge Protocol Data Units.
CISCO	Fabricante de dispositivo como conmutador y enrutador.
FIREWALL	Cortafuegos.
IDS	Sistemas de detección de intrusos.
IPS	Sistemas de prevención de intrusos.
LAN	Red de área local.
OSI	Interconexión de sistemas abiertos.
STP	Del inglés Spanning Tree Protocol.
VLAN	Red de área local virtual.
VTP	Del inglés Vlan Trunking Protocol.
WHITE-BOX	Caja blanca.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Este trabajo se basa en una problemática encontrada en las redes corporativas en lo referente a la seguridad de los dispositivos de capa 2 donde podemos evidenciar mediante el análisis los riesgos no contemplados al momento de la puesta en producción de esos dispositivos sin la debida evaluación de los riesgos y la aplicación de los controles necesarios para mitigarlos y así minimizar las vulnerabilidades en dichas redes.

En el desarrollo del trabajo vamos analizar las configuraciones de unos conmutadores CISCO que se encuentran en operación dentro de una infraestructura tecnológica y la ejecución de una herramienta que nos permite realizar una evaluación de las vulnerabilidades de los protocolos de capa de acceso.

En base al análisis y evaluación antes mencionada se procede a realizar un esquema funcional y aplicable permitiendo a los administradores de

conmutadores poder contar con un mecanismo fiable y sencillo el mismo que podrán seguir para contrarrestar las falencias detalladas en el análisis.

Durante la implementación del esquema en los dispositivos se corrige las frágiles configuraciones, robusteciendo la seguridad de la infraestructura ante los eminentes desafió que conlleva un ataque imprevisto a los conmutadores de la red.

Finalmente luego de la aplicación del esquema se realizara la validación de los resultados obtenidos y confirmando si el esquema es viable en la mejora de la seguridad de los conmutadores.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

En las empresas se ha observado últimamente todos los esfuerzos en la aplicación de los controles necesarios en su infraestructura tecnológica evitando que la información sea manipulada por terceros, instalando dispositivos como: firewall, ips, ids, antivirus, etc. y reforzando sus sistemas operativo o software empresariales evitando sean un objetivo fácil de cualquier usurpación de su información pero tomando como referencia el modelo OSI a nivel de capa 1 o 2 donde se puede generar un ataque de denegación de servicio no lo han considerado ponemos de ejemplo en capa 1 el impacto ante un desastre natural, daño eléctrico, o el daño por

roedores donde la disponibilidad operativa de estas empresas ha sido mermada dejando de trabajar por un tiempo considerable hasta restablecer nuevamente sus servicios.

A nivel de capa 2 la explotación de vulnerabilidad de los protocolos de capa 2:

- Protocolo de árbol de expansión (del inglés Spanning Tree Protocol, STP).
- Protocolo troncal de red de área local virtual (del inglés VLAN Trunking Protocol, VTP).

Donde el esquema integral de seguridad de las empresas deja por fuera estas capas permitiendo una brecha en la seguridad y facilitando al atacante realizar una denegación del servicio si llega a comprometer un conmutador de la red de área local.

A continuación detallamos la problemática encontrada.

- Credenciales de usuarios utilizadas en el conmutador son muy frágiles.
- Protocolo de conexión remota al conmutador es inseguro.
- Acceso al conmutador desde cualquier ubicación sin restricción.
- Puertos Ethernet del conmutador habilitados aunque no exista dispositivo conectado.
- Falta de asignación de redes de área local virtual para los puertos Ethernet no utilizados.
- Puertos Ethernet utilizados en el conmutador sin la debida protección ante un cambio del dispositivo que se encuentra conectado.
- Configuración incompleta en los puertos Ethernet troncales que participan de STP.
- Configuración incompleta en los puertos Ethernet de acceso que participan de STP.
- Protocolo troncal de VLAN sin contraseña.

1.2. Solución propuesta

En base a lo antes mencionado teniendo la referencia al problema planteado sugerimos contar con un esquema aplicable para el fortalecimiento de las características en los conmutadores CISCO que participan en la interconexión a nivel de capa 2 en una red de área local.

La propuesta de este proyecto de tesis se basa en los siguientes puntos a seguir:

- Credenciales de usuarios robustas y encriptados.
- Protocolo seguro para la conexión remota al conmutador.
- Implementación de lista de acceso al conmutador.
- Apagado de los puertos Ethernet no conectados del conmutador.
- Creación de una red de área local virtual para la asignación de los puertos Ethernet no utilizados.
- Habilitación de la opción puerto seguro en las interfaces Ethernet de acceso en el conmutador.

- Configuración de la protección de conmutador raíz en los puertos que participan de STP.

- Configuración de la convergencia rápida y protección BPDU en los puertos Ethernet de acceso que participan de STP.

- Configuración de una contraseña para el protocolo VTP.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 Análisis de las configuraciones de los conmutadores

Para los análisis previstos en el presente trabajo nos basamos en la evaluación White-Box por la cual se conoce las configuraciones de los conmutadores y el acceso a la infraestructura de red de la empresa a la cual evaluaremos, dichas configuraciones las encontramos en las siguientes figuras 2.1-3 y procederemos a realizar un reconocimiento pasivo de las credenciales de usuario y sus contraseñas comparando con el diseño de arquitectura CISCO [1] que los conmutadores dentro de sus configuraciones poseen una base local de usuarios con perfil de administrador y se evidencia que los mismos presentan sus contraseñas en texto plano y muy simple en estructura,

adicionalmente se realiza la verificación de la aplicación de un algoritmo de encriptación para proteger las contraseñas pero se observa que no se encuentran habilitados.

```
hostname PISO2LADO_A
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username cisco password 0 cisco2013
username admin password 0 admin123
username proyecto password 0 123456789
username temporal password 0 temporal
```

Figura 2. 1 Configuración conmutador PISO2LADO_A

```
hostname PISO2LADO_B
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username cisco password 0 cisco2013
username admin password 0 admin123
username proyecto password 0 123456789
```

Figura 2.2 Configuración conmutador PISO2LADO_B

```
hostname PISO1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username cisco password 0 cisco2013
username admin password 0 admin123
username proyecto password 0 123456789
```

Figura 2.3 Configuración conmutador PISO1

2.2 Análisis del mecanismo para la conexión remota de gestión en el conmutador

Continuando con el análisis de reconocimiento pasivo basado en las configuraciones proporcionadas se revisa el mecanismo vigente para la conexión remota hacia los conmutadores evidenciando que se lo realiza bajo un protocolo vulnerable además se lo puede ejecutar desde cualquier ubicación dentro de la infraestructura de red sin precautelar ni realizar algún tipo de control o registro.

Se evidencia que los puertos no utilizados de los conmutadores se encuentran encendidos permitiendo así conectividad a la red corporativa, al momento de conectar cualquier dispositivo estos se conectan a la VLAN por defecto además se observa que los puertos utilizados pueden ser fácilmente suplantados por otros dispositivos pues no cuenta con alguna protección de seguridad a nivel de puerto de acceso a continuación las figuras 2.4-6.

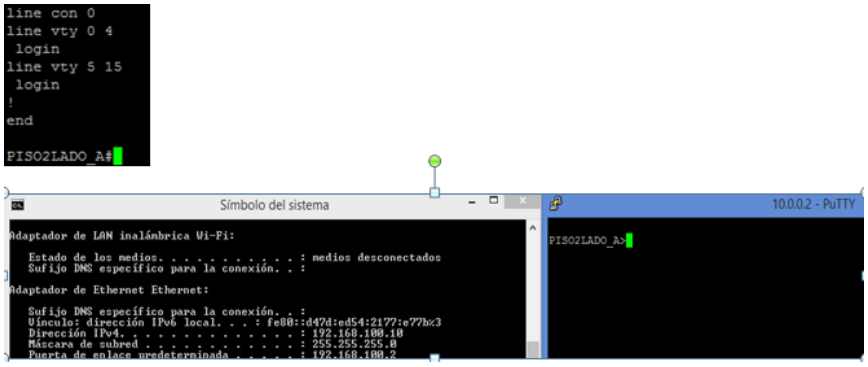


Figura 2.4 Conexión remota conmutador PISOLADO_A

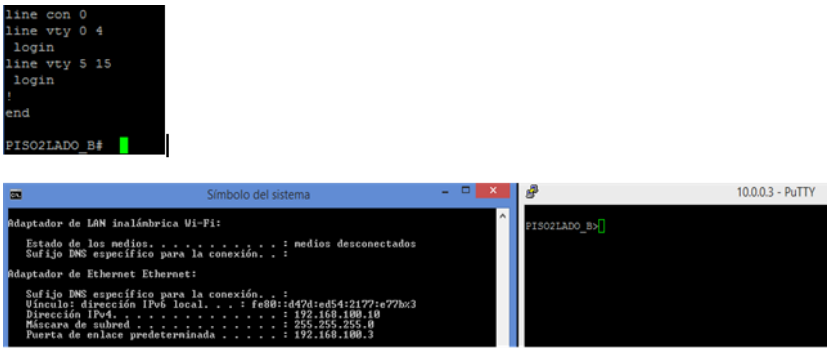


Figura 2.5 Conexión remota conmutador PISOLADO_B

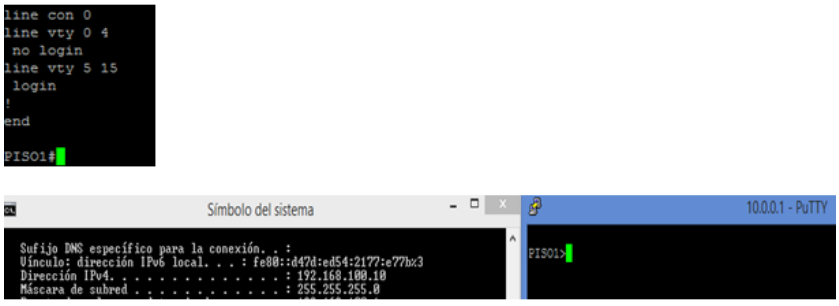


Figura 2.6 Conexión remota conmutador PISO1

2.3 Análisis de vulnerabilidad en los protocolos de capa 2 mediante el uso de la herramienta Yersinia

Para el análisis de los protocolos de capa 2 STP, VTP vamos a realizar un reconocimiento activo figura 2.7-8 mediante la utilización de una herramienta [5] instalada en un computador figura 2.9 y conectada a la red para generar un ataque a los protocolos de capa de acceso figura 2.10 y logrando de esa manera obtener las vulnerabilidades que puedan existir en los protocolos STP y VTP.

El resultado de la ejecución de la herramienta se detalla en la figura 2.11 en el cual nos arroja las vulnerabilidades en los protocolos antes indicados.

Podemos acotar que en el caso del protocolo STP se observa que los puertos de acceso no tienen las debidas configuraciones necesarias para evitar que otro conmutador ajeno a la infraestructura se instale y converge generando cambios en la topología de STP. Además se observa falta de configuración en los puertos troncales que son participe de la topología libre de lazo en capa de acceso.

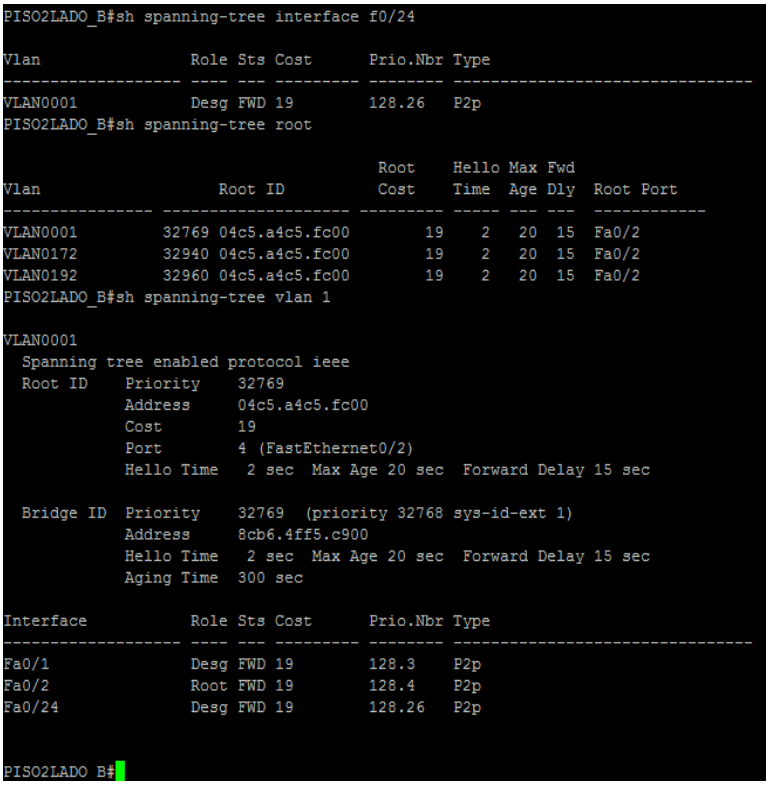


Figura 2.7 Puerto sin protección del conmutador PISO2LADO_B

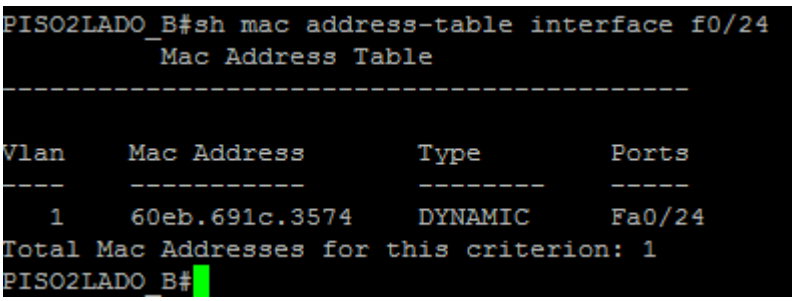


Figura 2.8 Dirección física en el puerto fa0/24 del conmutador PISO2LADO_B

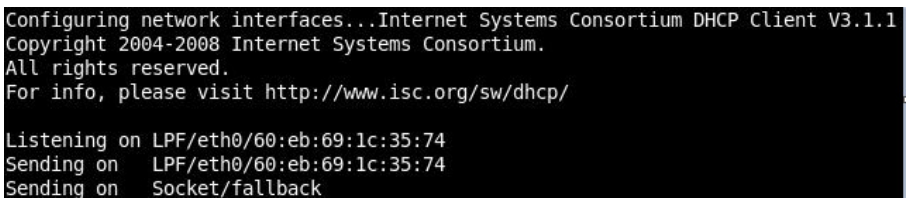


Figura 2.9 Dirección física del PC con Yersinia

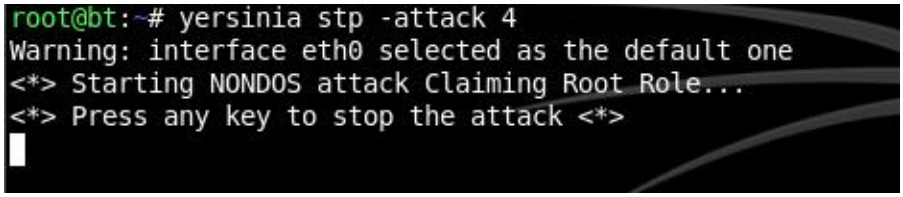


Figura 2.10 Ataque al protocolo STP utilizando la herramienta Yersinia

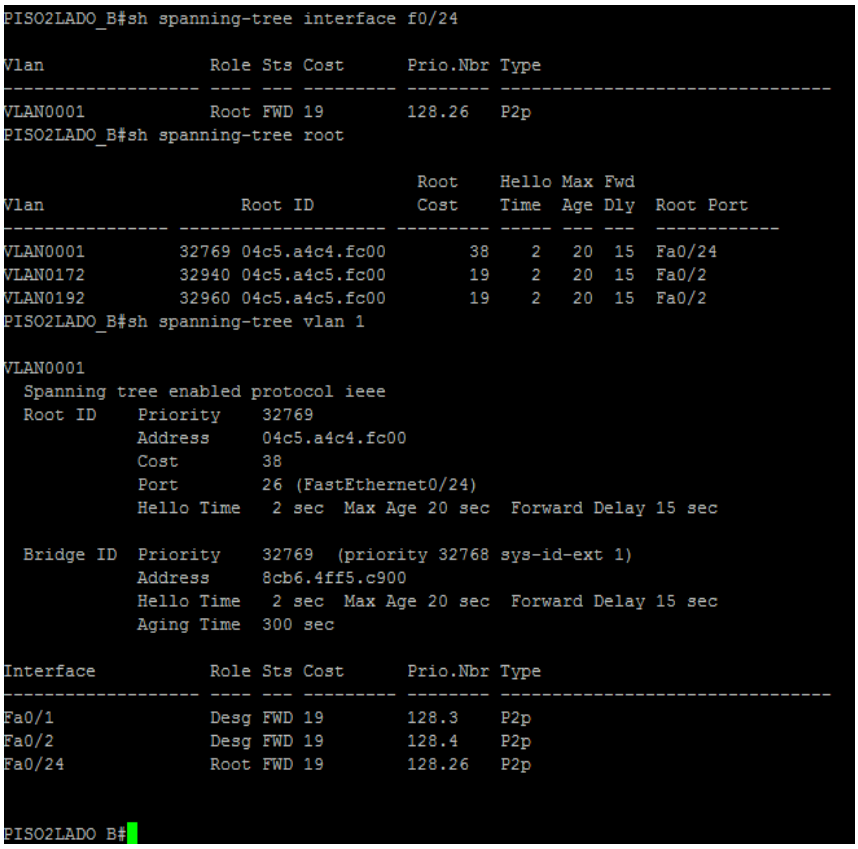


Figura 2.11 Resultado de las vulnerabilidades en STP en conmutador PISO2LADO_B

En lo referente al protocolo VTP se observa que las conversaciones entre los conmutadores no se encuentran debidamente protegidas figura 2.12 por lo cual un atacante puede aprovechar esa deficiencia y husmear dichas conversaciones de los conmutadores y manipular las

VLANs que se encuentran configuradas dentro de la infraestructura lo observamos en las figuras 2.13-16.

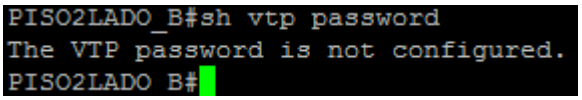


Figura 2.12 Protocolo VTP sin protección en conmutador PISO2LADO_B

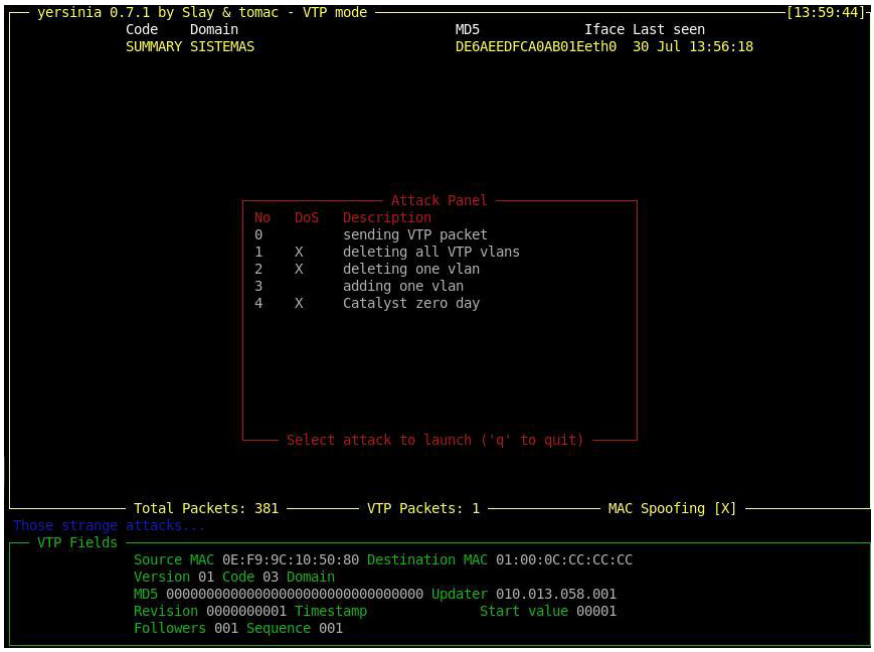


Figura 2.13 Fase 1 del ataque al protocolo VTP con herramienta Yersinia en conmutador PISO2LADO_B

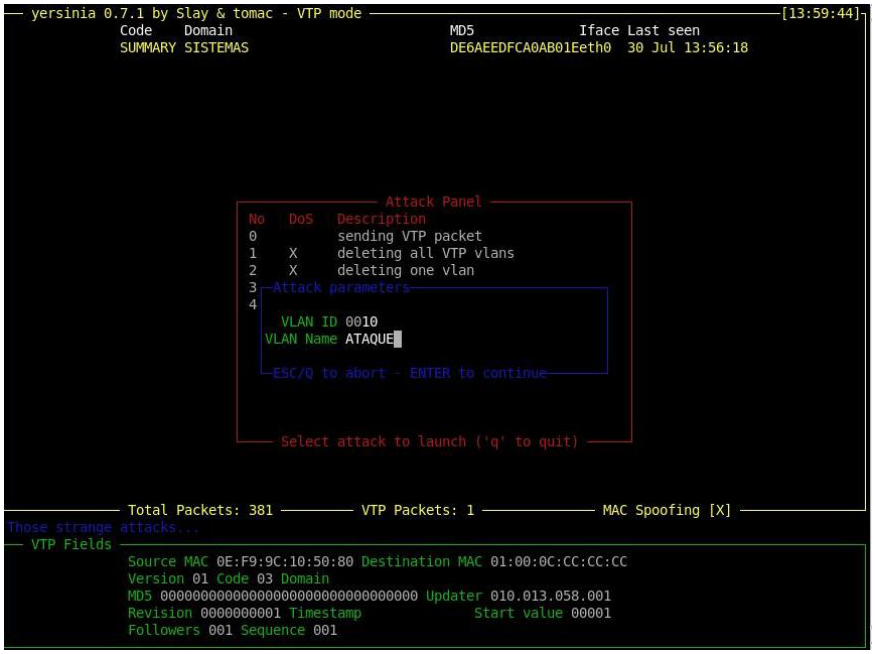


Figura 2.14 Fase 3 del ataque protocolo VTP con herramienta Yersinia en conmutador PISO2LADO_B

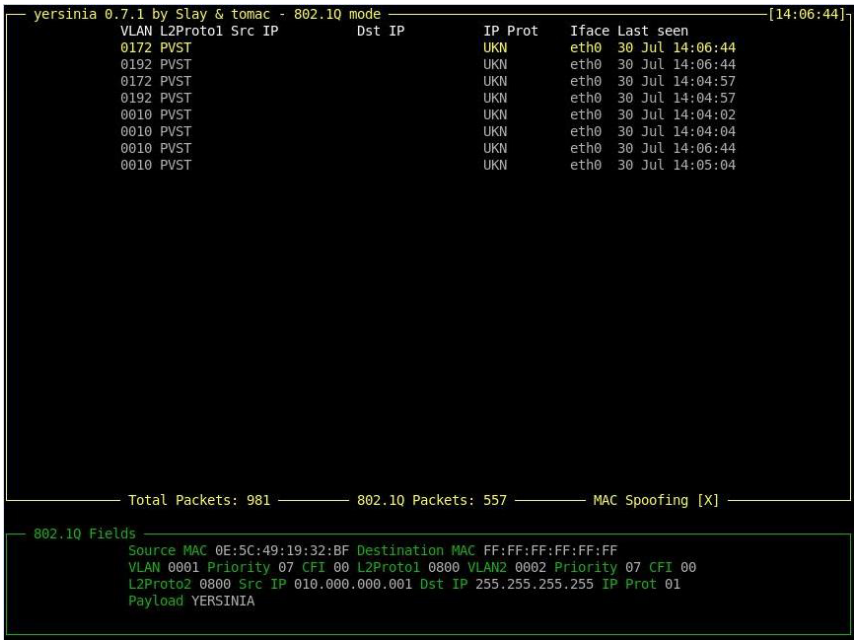
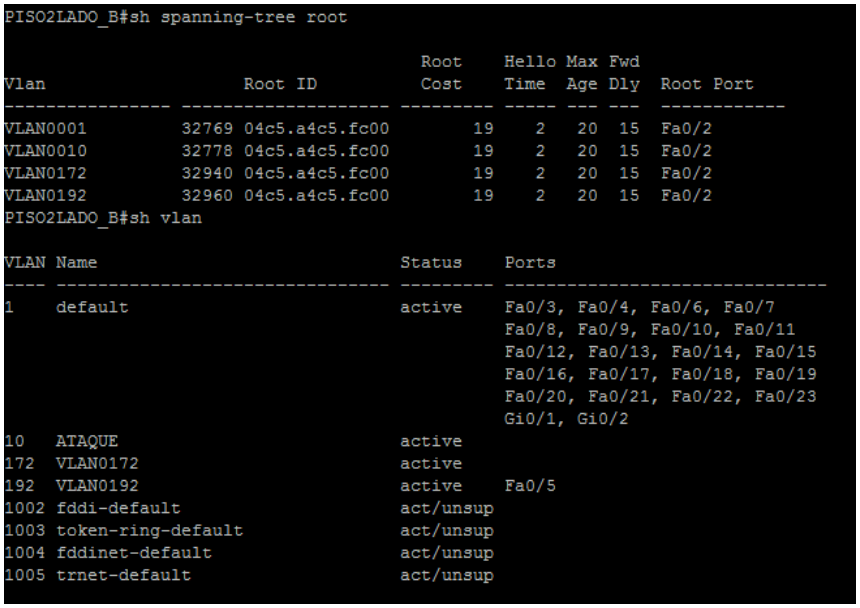


Figura 2.15 Fase 3 ataque en proceso en conmutador PISO2LADO_B



```
PISO2LADO_B#sh spanning-tree root

                                        Root    Hello Max Fwd
Vlan                Root ID             Cost    Time  Age Dly  Root Port
---------------- ------------------- --------- ----- --- ---  ------------
VLAN0001         32769 04c5.a4c5.fc00        19    2   20  15  Fa0/2
VLAN0010         32778 04c5.a4c5.fc00        19    2   20  15  Fa0/2
VLAN0172         32940 04c5.a4c5.fc00        19    2   20  15  Fa0/2
VLAN0192         32960 04c5.a4c5.fc00        19    2   20  15  Fa0/2
PISO2LADO_B#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gi0/1, Gi0/2
10   ATAQUE                            active
172  VLAN0172                          active
192  VLAN0192                          active    Fa0/5
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Figura 2.16 Resultados del ataque al protocolo VTP con herramienta Yersinia en conmutador PISO2LADO_B

2.4 Diseño de un esquema para reforzar la seguridad de manera integral en los conmutadores CISCO de capa 2 en la red de área local

Dentro del diseño para obtener un esquema estándar y factible de aplicarlo en los conmutadores de la infraestructura de red debemos basarnos en la normativa NTE INEN-ISO/IEC 27002:2005 [2], de la cual escogeremos algunos controles correspondiente a la parte de control de acceso los cuales se encuentran detallados en tabla 1.

Tabla 1 Controles de la normativa NTE INEN-ISO/IEC 27002:2005.

A.11 Control de acceso		
A.11.4 Control de acceso a la red		
A.11.4.1	Política de uso de los servicios en red	Control Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.
A.11.4.2	Autenticación de usuario para conexiones externas	Control Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.
A.11.4.3	Identificación de los equipos en las redes	Control La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones
A.11.4.4	Diagnostico remoto y protección de los puertos de configuración.	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.
A.11.5 Control de acceso al sistema operativo		
A.11.5.2	Identificación y autenticación de usuario	Control Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario.
A.11.5.3	Sistema de gestión de contraseñas	Control Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas de calidad.

En base a lo antes expuesto la estructura a cumplir dentro del esquema diseñado será el siguiente.

- Creación de usuario en base al rol para el mantenimiento del conmutador.
- Generación de contraseñas de usuarios robustas.
- Aplicación de algoritmo de encriptación en las contraseñas.

- Creación de usuario para las conexiones remotas.
- Aplicación de un protocolo seguro para la conexión remota al conmutador.
- Implementación de una lista de acceso restringiendo la comunicación hacia al conmutador.
- Control de los puertos Ethernet no conectados del conmutador.
- Creación de una VLAN para la asignación de los puertos Ethernet no utilizados.
- Aplicación de la opción puerto seguro en las interfaces Ethernet de acceso en el conmutador.
- Aplicación de la protección de conmutador raíz en los puertos que participan de STP.
- Aplicación de la convergencia rápida y protección BPDU en los puertos Ethernet de acceso que participan de STP.
- Generación de una contraseña para el protocolo VTP.

2.5 Implementación del esquema para reforzar la seguridad en los conmutadores CISCO de capa 2 en la red de área local

Durante la implementación del esquema propuesto en este trabajo debemos apoyarnos con la guía de comandos de los conmutadores CISCO [3] que tenemos en operación dentro de la infraestructura

tecnológica en este caso el modelo de conmutador utilizado en la red corporativa corresponde a CISCO Catalyst 3560.

Para la operativa de los conmutadores se van a configurar dos usuarios locales uno con el perfil de operador y el otro con el perfil de administrador, para lo cual nos basaremos en la guía de configuración de los conmutadores CISCO [4] que serán utilizados al momento de un mantenimiento o una resolución de problema y necesiten conectarse vía consola al dispositivo.

En lo concerniente a la conexión remota se configura un usuario local y se habilitara el servicio de SSH como único método de acceso remoto con un máximo 3 intentos de autenticación y solo podrán ser realizadas desde la red 10.0.0.0/24 cualquier otro origen será denegado para lo cual se implementa una lista de acceso estándar cualquier intento de conexión sea este permitido o denegado será ingresado al syslog dichos comandos los encontramos en la tabla 2.

Tabla 2 Comandos aplicados en conmutadores CISCO 3560

configure terminal
username operador privilege 7 secret 0pe1ad0R2015

username admin1 privilege 15 secret Adm1N2015
privilege exec level 7 show logging
privilege exec level 7 show running-config
privilege exec level 7 show
enable secret C1sc02015
service password-encryption
username soporte privilege 15 secret S0p0rtE2015
ip domain name empresa.com
crypto key generate rsa
1024
ip ssh authentication-retries 3
ip ssh logging events
ip ssh version 2
access-list 1 permit 10.0.0.0 0.0.0.255 log
access-list 1 deny any log
line con 0
login local
line vty 0 4
access-class 1 in
login local
transport input ssh

vlan 999
interface range fastEthernet 0/6-24
switchport mode access
switchport access vlan 999
Shutdown
interface range fastEthernet 0/3-5
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
Exit
Wr

2.6 Implementación de las configuraciones en los puertos de acceso y troncal que participan de STP

En la implementación de configuraciones en los puertos de acceso dentro del conmutador se procede a configurar lo siguiente: primero la transición inmediata del puerto al estado de reenvió y segundo si reciben BPDU en un puerto de acceso el mismo se vaya automáticamente a deshabilitado hasta que el administrador de

manera manual nuevamente habilite el puerto dichos comandos los encontramos en la tabla 3.

Tabla 3 Comandos para configuración de portfast

configure terminal
spanning-tree portfast default
spanning-tree portfast bpduguard default
Wr

En el caso del puerto troncal se implementa las siguientes configuraciones para evitar que otro conmutador tome el rol de raíz y también evitar se genere un lazo cuando no se recibe un BPDU en un puerto que lo está esperando, lo comandos utilizados los proporcionamos en la tabla 4.

Tabla 4 Comandos para configurar loopguard

configure terminal
spanning-tree loopguard default
Wr

Solo para el caso de un conmutador raíz se procede con los siguientes comandos mostrados en la tabla 5.

Tabla 5 Comando para configurar guard

configure terminal
interface range fastEthernet 0/1-2
spanning-tree guard root
Exit
Wr

2.7 Implementación de contraseña en el VTP

Para la implementación de este punto vamos utilizar el algoritmo criptográfico MD5 para asegurar todas las actualizaciones VTP mediante la siguiente contraseña S1stema? los comandos utilizados son los detallados en la tabla 6.

Tabla 6 Comando para configurar VTP

configure terminal
vtp version 2
vtp password S1stema?
exit
wr

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Interpretación de los resultados en base al análisis realizado mediante la herramienta Yersinia posterior a la implementación

Luego de aplicar las implementaciones antes indicada en el presente trabajo tenemos como resultado que las vulnerabilidades encontradas en los conmutadores para los protocolos STP y VTP que conllevaban un riesgo para la seguridad en la infraestructura fueron controladas y minimizadas evitando su accionar al momento de un ataque, por lo cual se fortaleció la seguridad de los dispositivos, con esto salvaguardamos que no cambie la topología libre de bucle y que se eliminen o creen VLAN dentro de los conmutadores.

3.2 Validación de credenciales de usuarios seguras

Dentro de este punto procedemos a evidenciar que luego de aplicar las configuraciones indicadas en el capítulo anterior ya no se puede obtener de manera visual dentro de las configuraciones de los conmutadores las contraseñas de los usuarios locales el mismo que se detalla en las figuras 3.1 -3.

```
hostname PISO1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$c2H6$IpUd3NjxHqtaS1P89MaWU1
!
username admin password 7 011202095205575D72
username operador privilege 7 secret 5 $1$JuCQ$oIzFh5xcdlhUBO9rY.0.3/
username admin1 privilege 15 secret 5 $1$lLrB$EaAZKi3n3C/ST/ik05swv0
username soporte privilege 15 secret 5 $1$g4vI$0dtI6exmCvn0rzvbdNvC00
```

Figura 3.1 Credenciales encriptadas en conmutador raíz

```
hostname PISO2LADO_A
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$NMHY$4kzZ2fhbcn/mdn6wielmA0
!
username operador privilege 7 secret 5 $1$QVxi$qHfEjPbORvH/U9/1SqZSi0
username admin1 privilege 15 secret 5 $1$dw8O$5gi6NKzlXAPNsxrrujmdx/
username soporte privilege 15 secret 5 $1$OLFL$/.U6aqa3wBpxrQK4sPVM/1
```

Figura 3.2 Credenciales encriptadas en conmutador PISO2LADO_A

```
hostname PISO2LADO_B
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9OUx$j/v6zjCZ3k4KXIXtjz2H8.
!
username operador privilege 7 secret 5 $1$r17s$yhacr253F3XIdg.M0dhrM1
username admin1 privilege 15 secret 5 $1$Y5SV$1IYBNRtvURfccK5U6PM591
username soporte privilege 15 secret 5 $1$jGWT$ZAAbrZ8.q08fk7dE4kCcB1
```

Figura 3.3 Credenciales encriptadas en conmutador PISO2LADO_B

3.3 Validación de la conexión remota de gestión

Luego de la implementación procedemos a realizar intentos de conexión por un protocolo inseguro y observamos que el mismo no se encuentra habilitado y luego se procede con la conexión segura pero desde una ubicación no permitida evidenciando que ambos casos ya están controlados por la configuración realizada a continuación la figura 3.4 y 3.5.

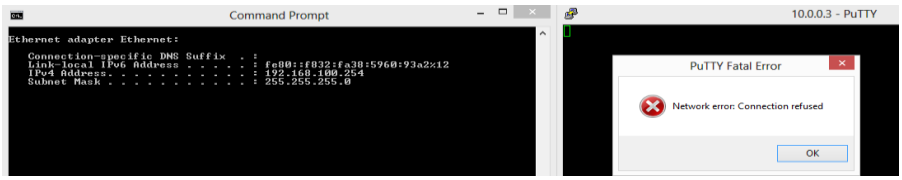


Figura 3.4 Validación de conexión remota en conmutador PISO2LADO_B

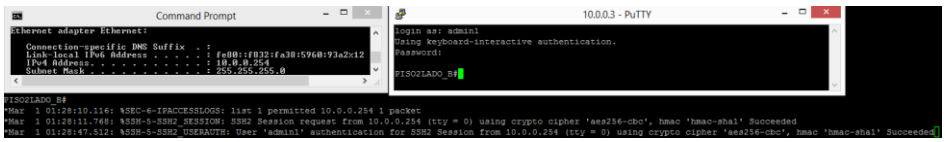


Figura 3.5 Syslog de evidencia de conexión remota por protocolo seguro

3.4 Validación de los puertos seguros en el conmutador

Para esta validación se utiliza dos computadoras la primera al momento de conectarla al conmutador se obtiene la MAC y el puerto está habilitado como muestra la figura 3.6, luego se procede a conectar la segunda computadora en el mismo puerto del conmutador y la protección del mismo genera que el puerto se deshabilite como muestra la figura 3.7.

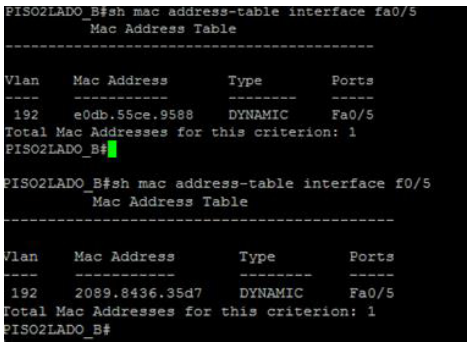


Figura 3.6 Carencia de control en los puertos de acceso

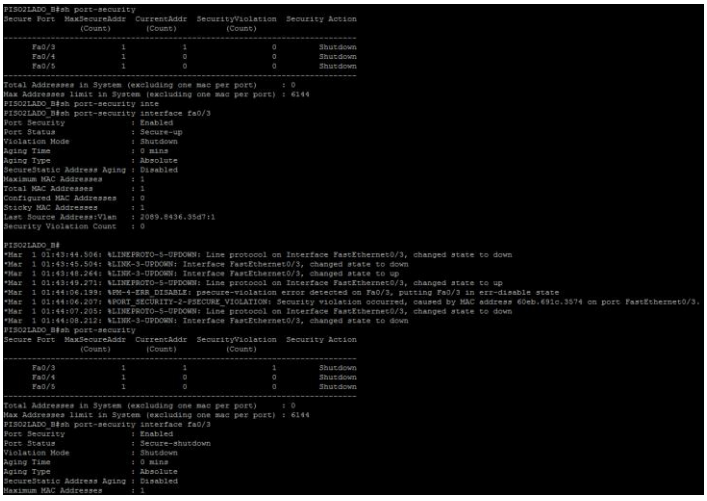


Figura 3.7 Aplicación de seguridad en los puertos de acceso en conmutador PISOLADO_B

3.5 Validación de los protocolos STP, VTP

Para esta validación procedemos a conectar un conmutador en un puerto de acceso para evidenciar que el mismo antes de implementar el esquema de seguridad es vulnerado se demuestra en las figuras 3.8-10 luego que se activa su protección utilizamos el Yersinia para simular un conmutador raíz pero el ataque no es exitoso pues deshabilita el puerto, luego procedemos a generar que otro conmutador dentro de la topología intente asumir el rol de raíz a través de Yersinia para observar el comportamiento del puerto troncal capturado en las figuras 3.11-12, y por la validación del VTP podemos observar la figura 3.13 donde el ataque no es exitoso.

```
PISO1#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0172, VLAN0192
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          2          2
VLAN0172                    0         0        0          2          2
VLAN0192                    0         0        0          3          3
---------------------- -------- --------- -------- ---------- ----------
3 vlans                     0         0        0          7          7
PISO1#
```

Figura 3.8 Conmutador raíz actual

```
PISO3#sh run | i span
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,172,192 priority 24576
PISO3#
```

Figura 3.9 Conmutador con mejor prioridad en STP

```
PISO1#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          3          3
VLAN0172                      0         0        0          3          3
VLAN0192                      0         0        0          4          4
---------------------- -------- --------- -------- ---------- ----------
3 vlans                       0         0        0         10         10
PISO1#
```

Figura 3.10 Cambio de rol del conmutador raíz

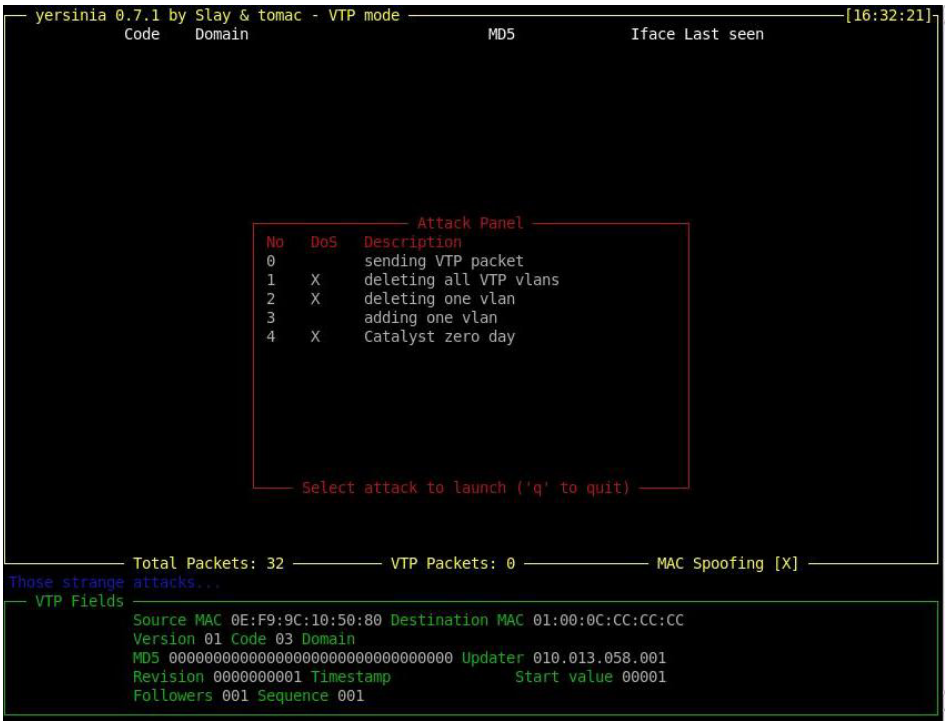


Figura 3.11 Fase 1 del nuevo ataque al protocolo VTP mediante herramienta Yersinia

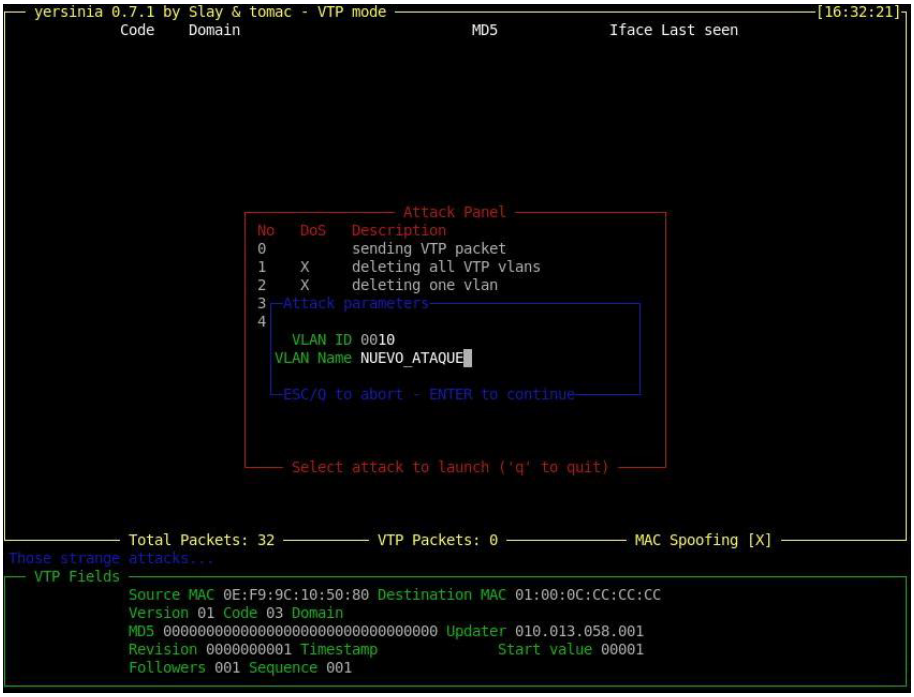


Figura 3.12 Fase 2 del nuevo ataque de protocolo VTP mediante herramienta Yersinia

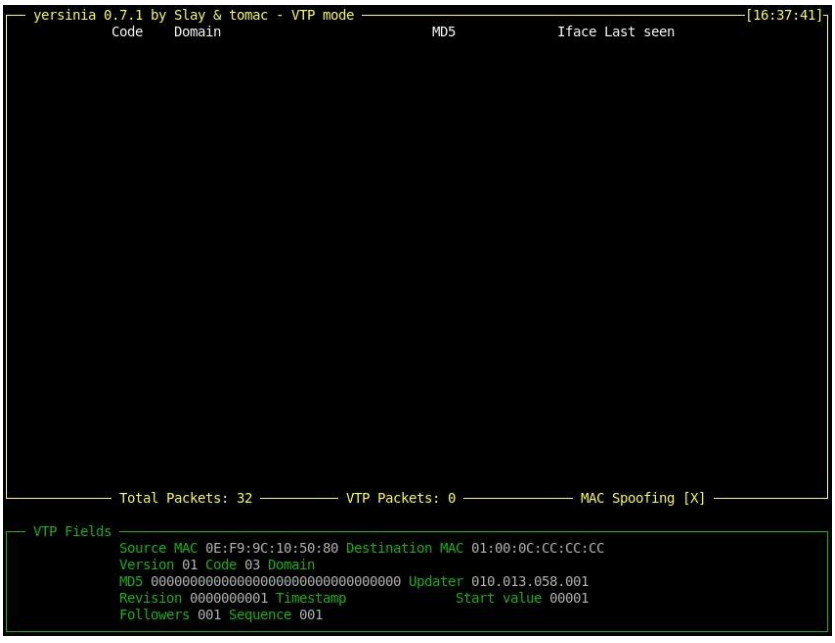


Figura 3.13 Validación de protección de protocolo VTP

CONCLUSIONES Y RECOMENDACIONES

1. Podemos concluir que dentro de la infraestructura tecnológica los conmutadores son dispositivos poco considerando en el esquema de seguridad de la información en algunas empresas.

2. Los administradores de dichos dispositivos no están consienten de la importancia de contar con los controles necesarios para contrarrestar un eminente ataque a la infraestructura tecnológica.

3. Contar con un esquema aplicable en las configuraciones de los conmutadores para robustecer su seguridad y desempeño en la red

corporativa y que sea un estándar para futuras nuevas incorporaciones de dispositivos en la red.

4. Evitar que dispositivos que se encuentran en operación dentro de una infraestructura tecnológica mantengan configuraciones sencillas y vulnerables.

BIBLIOGRAFÍA

[1] Cisco System, Designing Cisco Network Service Architectures, CISCO, 2012.

[2] NTE INEN-ISO/IEC 27001:2011, Tecnología de la información - Técnicas de seguridad - Sistema de Gestión de la seguridad de la información (SGSI) - Requisitos, 2011, Página 24.

[3] Cisco System, Catalyst 3560 Switch Command Reference, CISCO, 2013.

[4] Cisco System, Catalyst 3560 Switch Software Configuration Guide, CISCO, 2013.

[5] Alfredo Omella y David Barroso, Yersinia, http://www.yersinia.net/, 2006.