Tendencias de la educación en seguridad

Laboratory for Vulnerability Analysis and CIS Controls on Layer 2 Switches

William-Rogelio Marchand-Niño[1]
william.marchand@unas.edu.pe

José Martin Santillan Ruiz[1]
jose.santillan@unas.edu.pe

***Resumen*— En el proceso de enseñanza de temas relacionados con la seguridad de la red, es importante que el estudiante tenga un enfoque más real de las vulnerabilidades y los tipos de ataques que pueden especificarse en los entornos de red de producción de infraestructuras de Tecnologías de Información y Comunicación. El objetivo principal es proporcionar al alumno escenarios que le permitan llevar a cabo un análisis de vulnerabilidad completo, desde la identificación de la vulnerabilidad, explotación o verificación de la vulnerabilidad con técnicas de *hacking* ético, evaluación CVSS, mitigación y alineación con algún control de CIS (*Center of Internet Security*). El Laboratorio propuesto es una forma de apoyo para el proceso de enseñanza-aprendizaje de la seguridad de la red a nivel universitario. Ofrece un paquete práctico que incluye las fases generales y comunes de un ataque (enfoque de seguridad ofensiva), procedimientos de mitigación (enfoque de seguridad defensiva) y controles de seguridad basados en una referencia válida como CIS (gestión de seguridad informática).**

***Palabras clave*— Vulnerabilidades, *pentesting*, redes, CIS, CVSS, capa dos OSI, amenazas, seguridad ofensiva, aprendizaje.**

I. INTRODUCCIÓN

La investigación está orientada a la propuesta de un Laboratorio para el análisis de las vulnerabilidades asociadas a la deficiente configuración de los dispositivos de red de capa 2, específicamente los conmutadores (switches) de red. La deficiente configuración o las omisiones en las misma, también se debe al efecto de crecimiento de la red, al incrementarse el número de dispositivos, también se incremente el volumen de configuraciones, y esto genera que las amenazas (de reconocimiento, acceso o denegación de servicio) puedan concretarse en ataques o incidentes de seguridad no deseados dañando a los sistemas u organización. [1] [2] [3].

Para la definición del alcance del Laboratorio se identificó las principales vulnerabilidades que presentan comúnmente los dispositivos de capa de enlace de datos, tomando como referencia la base de datos de dominio público CVE (Common Vulnerabilities and Exposures) siendo algunas de estas, ARP spoofing, salto de VLAN, ataques de fuerza bruta o diccionario contra servicios TELNET y SSH, ataques de hombre-en-el-medio, DHCP spoofing y claim role STP forman parte de las pruebas de concepto con los recursos disponibles para el montaje de un Laboratorio orientado al estudio de seguridad de redes [4] [5] [6]. Asimismo, se consideró incluir la valoración del grado de severidad que está de acuerdo con el Sistema de Calificación de Vulnerabilidades Comunes (CVSS) [7]. El objetivo principal es proveer al estudiante escenarios que pueden presentarse en entornos de producción y realizar un análisis de vulnerabilidades completo, desde la identificación de la vulnerabilidad, explotación o verificación de la vulnerabilidad con técnicas de ethical hacking (enfoque de seguridad ofensiva), valoración CVSS, mitigación (enfoque de seguridad defensiva), y alineación con los 20 controles (enfoque de la gestión de seguridad informática) críticos de CIS (Center for Internet Security) [8].

Para el desarrollo del Laboratorio se ha formulado una rubrica asociada para la verificación del cumplimiento de los pasos formulados.

Una característica para resaltar de la propuesta de este Laboratorio es su forma de aplicación, que está orientada a un tipo de desafío o CtF (Capture the Flag) con formación de equipos, que en otros estudios muestran un impacto positivo, lo que indica en principio, que es un método efectivo para afianzar las capacidades y habilidades en temas relacionados a la seguridad informática, promoviendo el trabajo en equipo, la colaboración y la competencia [9].

La práctica de evaluar o diagnosticar el nivel de seguridad de una red debe ser una práctica común y frecuente, porque a pesar que los sistemas puedan tener instalado las últimas actualizaciones no significa que están libres de vulnerabilidades, por el contrario, se evidencia que las deficientes configuraciones son causa de vulnerabilidades que son aprovechadas por los actores de amenaza [10].

Una de las formas de evaluar la robustez de la infraestructura es sometiendo a prueba las defensas implementadas a nivel de configuraciones y servicios habilitados en los equipos de red. Uno de los beneficios de utilizar pruebas de penetración en el contexto de la seguridad informática es que esta provee de un enfoque desde la perspectiva de un atacante real que dirige técnicas de explotación para romper la protección de un sistema [11] [12].

A nivel de los switches que operan en la capa de enlace de datos de acuerdo al modelo de referencia OSI, se establece algunos de los ataques más frecuentes dirigidos a este tipo de equipos, entre los que destacan, saturación de direcciones MAC, aprovechamiento de protocolos de descubrimiento, suplantación de identidad de switch, ataque de etiquetado doble, y la denegación de servicio [13] [14], que a su vez están relacionados a los siguientes tipos de vulnerabilidades:

- Imperfecciones en las políticas.
- Errores de diseño
- Deficiencias de protocolos
- Deficiencias en la configuración

[1] Grupo de Investigación en Redes, Seguridad y Gestión de TI
Universidad Nacional Agraria de la Selva - Tingo María, Perú

https://doi.org/10.12804/si9789587844337.18

- Debilidades en el software
- Factores humanos
- Software malicioso
- Vulnerabilidades de hardware
- Acceso físico a los recursos de red.
- Cifrado y autenticación

De la relación anterior y para efectos del trabajo de investigación, se consideran las siguientes:

- Deficiencias de protocolos
- Deficiencias en la configuración
- Cifrado y autenticación.

La fase de explotación en el contexto de las pruebas de penetración es la aplicación de exploits para lograr el acceso a los sistemas de un cliente. También es aprovechar las vulnerabilidades identificadas previamente, es la real fase de ataque. No es necesario utilizar exploits (código malicioso) para realizar el proceso de explotación. Otra definición de la explotación es el aprovechamiento de los fallos lógicos de los sistemas informáticos para lograr acceso privilegiado a la red, extraer información sensible o persistencia de ataque, mediante herramientas o técnicas de explotación como ataques de fuerza bruta o diccionario, ejecución de código, ingeniería social, pivoting, etc. [15] [16] [17].

Al realizar la explotación de vulnerabilidades se pueden utilizar herramientas automatizadas, sin embargo, se debe tener conciencia y certeza de lo que realmente está ejecutando el código de la herramienta o exploit. Muchas veces la automatización hace que el pentester pierda cierto control sobre el proceso de explotación, por lo que un pentester debe conocer y tener certeza de lo que se ejecuta y el tipo de vulnerabilidad que se está analizando [18].

En el aspecto de formas de mitigación, las soluciones propuestas en la literatura para enfrentar los ataques y amenazas en redes LAN Ethernet abarcan entre otros, el reemplazo de switch por router; protección física, segmentación VLAN; control de acceso de host basado en autenticación 802.1x; listas de control de acceso; seguridad de puerto; protección de sobrecarga, seguridad centralizada, protocolos seguros; monitorización de seguridad; además de corregir errores cometidos por parte de los administradores en los procedimientos de configuración [19].

La valoración de las vulnerabilidades se realizó utilizando la calculadora de CVSS versión 3 que tiene las siguientes métricas base [7]:

- Vector de Ataque (AV): Red, Adyacente, Local, Físico.
- Complejidad de Ataque (AC): Bajo, Alto.
- Privilegios Requeridos (PR): Ninguno, Bajo, Alto.
- Interacción con Usuario (UI): Ninguno, Requerido.
- Alcance (S): Sin cambios, cambiado.
- Confidencialidad (C): Ninguno, Bajo, Alto
- Integridad (I): Ninguno, Bajo, Alto.
- Disponibilidad (A): Ninguno, Bajo, Alto.

El resultado de la valoración estable una clasificación del nivel de severidad de la vulnerabilidad que se muestra en la Tabla I.

TABLA I. NIVELES DE SEVERIDAD CVSS

Nivel de severidad de vulnerabilidad	Puntuación CVSS
Ninguno	0.0
Bajo	0.1 – 3.9
Medio	4.0 – 6.9
Alto	7.0 – 8.9
Crítico	9.0 – 10.0

II. TIPOS DE ATAQUES PARA VULNERABILIDADES CONTRA SWITCHES

Algunos tipos de ataques o pruebas de concepto asociadas se describen a continuación:

A. Suplantación de identidad de DHCP.

DHCP es el protocolo que asigna automáticamente una dirección IP válida de un pool de DHCP a un host. Se pueden realizar dos tipos de ataques DHCP a una red conmutada: los ataques de agotamiento de DHCP y los de suplantación de identidad de DHCP.

En los ataques de suplantación de identidad de DHCP, un atacante configura un servidor de DHCP falso en la red para asignar direcciones de DHCP para los clientes. El motivo común de este ataque es obligar a los clientes a que usen servidores de Sistema de nombres de dominios (DNS) o de Servicio de nombres Internet de Windows (WINS) falsos y hacer que los clientes usen al atacante, o una máquina controlada por el atacante como gateway predeterminado.

B. Aprovechamiento de CDP

El Protocolo de Descubrimiento de Cisco (CDP, Cisco Discovery Protocol) es un protocolo propiedad de Cisco que puede configurarse en todos los dispositivos de este fabricante. CDP detecta otros dispositivos de Cisco conectados directamente, lo que permite que los dispositivos configuren su conexión de forma automática. En algunos casos, esto simplifica la configuración y la conectividad.

De manera predeterminada, la mayoría de los routers y switches Cisco poseen CDP habilitado en todos los puertos. La información de CDP se envía en broadcast periódicas sin cifrar. Esta información se actualiza localmente en la base de datos de CDP de cada dispositivo. Debido a que CDP es un protocolo de capa 2, los routers no propagan los mensajes CDP.

El protocolo análogo al CDP es el protocolo LLDP (Link Layer Discovery Protocol) que tiene funciones similares de descubrimiento de dispositivos a nivel de capa de enlace de datos. Este protocolo a diferencia de CDP es "multivendor", es decir opera de forma independiente a la marca del dispositivo.

El aprovechamiento de CDP se asocia a la divulgación información por la operación del protocolo en los puertos en los que no debería estar activo, y desde el punto de vista de los actores de amenazas se denomina un ataque reconocimiento.

Para efectos de las pruebas y por disponibilidad de equipos Cisco se utilizó el protocolo CDP.

C. *Ataque de suplantación de identidad de Switch*

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

Los saltos de VLAN permiten que una VLAN pueda ver el tráfico de otra VLAN. La suplantación de identidad de switch es un tipo de ataque con salto de VLAN que funciona mediante el aprovechamiento de un puerto de enlace troncal mal configurado. De manera predeterminada, los puertos de enlace troncal tienen acceso a todas las VLAN y pasan el tráfico para varias VLAN a través del mismo enlace físico, generalmente entre switches.

D. *Ataque de etiquetado doble*

Este tipo de ataque aprovecha la forma en que funciona el hardware en la mayoría de los switches. La mayoría de los switches realizan solo un nivel de desencapsulación 802.1Q, lo que permite que un atacante incorpore una etiqueta 802.1Q oculta en la trama. Esta etiqueta permite que la trama se reenvíe a una VLAN que la etiqueta 802.1Q original no especificó. Una característica importante del ataque con salto de VLAN de encapsulado doble es que funciona incluso si se inhabilitan los puertos de enlace troncal, ya que, generalmente, un host envía una trama por un segmento que no es un enlace troncal.

Los ataques con salto de VLAN de etiquetado doble implican los siguientes tres pasos:

- El atacante envía una trama 802.1Q con doble etiqueta al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal. Se supone que el switch procesa la trama que recibe del atacante como si estuviera en un puerto de enlace troncal o un puerto con una VLAN de voz (un switch no debe recibir una trama de Ethernet etiquetada en un puerto de acceso). Por ejemplo, suponga que la VLAN nativa es la VLAN 10. La etiqueta interna es la VLAN víctima; en este caso, la VLAN 20.
- La trama llega al switch, que observa la primera etiqueta 802.1Q de 4 bytes. El switch observa que la trama está destinada a la VLAN 10, que es la VLAN nativa. El switch reenvía el paquete por todos los puertos de la VLAN 10 después de eliminar la etiqueta de VLAN 10. En el puerto de enlace troncal, se elimina la etiqueta de VLAN 10, y no se vuelve a etiquetar el paquete porque esta forma parte de la VLAN nativa. En este punto, la etiqueta de VLAN 20 sigue intacta, y el primer switch no la inspeccionó.
- El segundo switch observa solo la etiqueta 802.1Q interna que envió el atacante y ve que la trama está destinada a la VLAN 20, el objetivo. El segundo switch envía la trama al puerto víctima o lo satura, según si existe una entrada en la tabla de direcciones MAC para el host víctima.

Este tipo de ataque es unidireccional y solo funciona cuando el atacante se conecta a un puerto que reside en la misma VLAN que la VLAN nativa del puerto de enlace troncal.

III. METODOLOGÍA

En esta sección se detallará el proceso de las pruebas de concepto, la valoración y mitigación asociada con los controles de CIS.

Para el montaje del Laboratorio se utilizaron los siguientes equipos:

- 3 switches Cisco Catalyst 2960 con IOS versión 12.
- Servidor de pruebas con sistema operativo Linux Ubuntu 16.04
- Dos máquinas virtuales con sistema operativo Windows 7. (víctimas)
- Una máquina virtual con sistema operativo Kali Linux 2018. (atacante)

El proceso de desarrollo de pruebas de concepto se realizó sobre una topología básica de experimentación con los equipos indicados anteriormente. La topología se muestra en la Fig. 1.

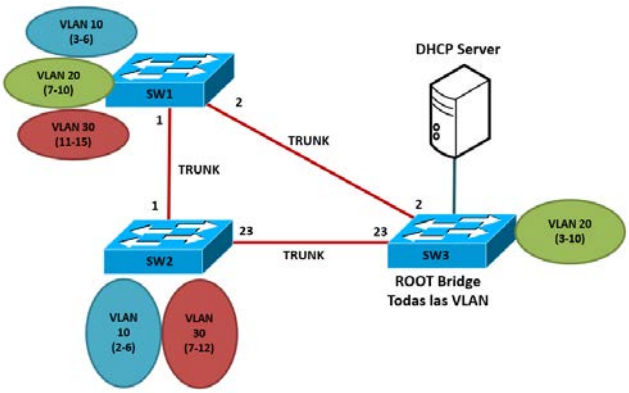

Fig. 1. Topología base para las Pruebas de Concepto.

De acuerdo con las vulnerabilidades comunes para los equipos de la capa de enlace de datos se definieron las pruebas específicas mostradas en la Tabla I.

TABLA II. PRUEBAS DE CONCEPTO

Protocolo	Prueba de Concepto
STP	*Claim root role*
CDP	Aprovechamiento de CDP
IEEE 802.1q	Salto de VLAN Aprovechamiento DTP
Telnet y SSH	Ataque de fuerza bruta
DHCP	Suplantación de servidor DHCP
ARP	ARP Posoning, *Man-in-the-middle*

Las herramientas para las pruebas son provistas por los instructores o docentes, entre las que destaca el framework Yersinia, que es un programa de software para realizar ataques (en nuestro caso pruebas de concepto) contra servicios y

protocolos de red tales como STP, CDP, DTP, DHCP, HSRP, 802.1Q y VTP. Estos ataques son realizados a nivel de capa 2.

El desarrollo del laboratorio se ejecuta en un contexto de tipo CtF (Capture the Flag) por equipos, con el propósito de promover la competencia y fortalecimiento de habilidades de concentración y trabajo en equipo.

En los escenarios planteados se asume que el atacante se encuentra en el mismo segmento de red que los dispositivos vulnerables, por lo que la evaluación y medición de los niveles de severidad son considerando este aspecto de ubicación del atacante.

Asimismo, es necesario considerar que los estudiantes al recibir entrenamiento sobre la metodología y el uso de herramientas de hacking están comprometidos con aspectos éticos y legales por lo que deberán firmar un Acuerdo de Compromiso sobre el uso adecuado de los conocimientos y herramientas a recibir. La finalidad es comprometer al estudiante a no usar el conocimiento adquirido para acciones fuera de la ley o ética. También se deberá emitir un "Disclaimer" sobre las técnicas mostradas.

En general las fases de desarrollo del Laboratorio son las siguientes:

- **Identificación de vulnerabilidad**. Este procedimiento es abierto a otras técnicas o formas de encontrar una vulnerabilidad, inclusive las herramientas (legales y éticas) a utilizar. El estudiante no queda limitado a una sola forma de proceder. Lo que se muestra en este trabajo es finalmente un ejemplo de un procedimiento clásico.
- **Verificación de vulnerabilidad**. Luego de identificar una vulnerabilidad se debe procede a comprobarla, es decir determinar si efectivamente es una vulnerabilidad que es susceptible de ser explotada o aprovechada. Las técnicas y herramientas son sugeridas, pero no quedan limitadas a esas.
- **Valoración CVSS.** En esta fase se debe estimar el grado de severidad de la vulnerabilidad que permite el ataque exitoso. Para la valoración se determina con el uso de la calculadora de CVSS versión 3.
- **Mitigación de la vulnerabilidad**. El estudiante deberá plantear las recomendaciones de mitigación asociadas a las soluciones que hayan determinado los fabricantes, sin embargo, no queda limitado a ese aspecto, por lo que el estudiante puede generar propuestas de mitigación diversas pero que deberá mostrar su eficiencia.
- **Alineación con los controles CIS.** En esta última fase el estudiante deberá analizar la correspondencia entre la vulnerabilidad de la prueba de concepto desarrollada con algún o algunos controles que CIS ha formulado.

A. Prueba de concepto de Claim Root Role

Sobre la topología base, se realizó la configuración de STP, definiendo a uno de los switches en el rol de "puente raíz" (root bridge) modificando la prioridad asociada. La Fig. 2 muestra el escenario.

La prueba de *Claim Root Role* consiste en la posibilidad de obtener el rol de Root para una topología conmutada con el protocolo Spanning Tree activo. El efecto de este ataque es desestabilizar o modificar la topología STP de la red, lo cual puede llevar a errores de control de bucles de forma intermitente; así como aprovechar el rol de puente raíz (root bridge) para otros ataques como denegación de servicio y man-in-the-middle.

Para esta prueba de ataque se utilizó la herramienta Yersinia, y se intentó obtener el rol de root en la VLAN 20, asumiendo que un atacante malicioso logre conectarse físicamente a un puerto de swtich en la VLAN 20. La valoración de la vulnerabilidad se muestra en la Tabla II.

Para mitigar el ataque se deben habilitar la siguiente configuración en los switches de la red:

```
S(config)#spanning-tree portfast bpduguard
```

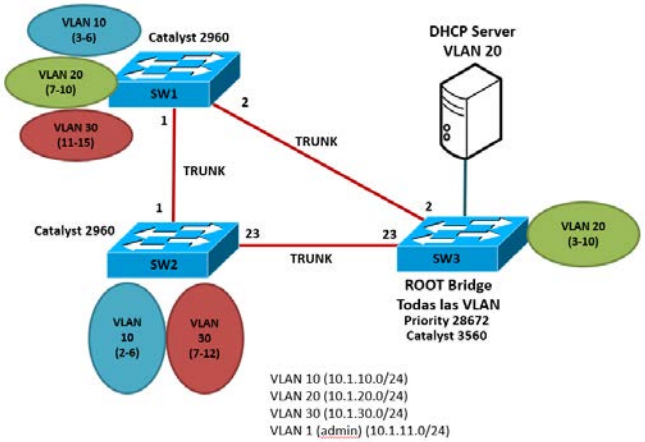

Fig. 2. Topología Pruebas de Concepto de Claim Root Role

TABLA III. VALORACIÓN CVSS DE CLAIM ROOT ROLE

Métrica Base	Valor
Vector de ataque	Adyacente
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguno
Alcance	Sin cambios
Confidencialidad	Ninguno
Integridad	Ninguno
Disponibilidad	Bajo
Puntuación Base CVSS v3.0	**4.3**

La Tabla III muestra el resultado de la valoración del nivel de severidad CVSS para el ataque de Claim Root Role que se establece en 4.3 como nivel medio, debido a que el vector de ataque es de modo adyacente, significa que se necesita estar en el mismo dominio de broadcast para explotar la vulnerabilidad, además de solo afectar a la disponibilidad de una forma baja.

B. Prueba de concepto de aprovechamiento de CDP

El protocolo CDP, propietario de Cisco, tiene la función de mantener informado a los equipos vecinos acerca del tipo de dispositivo conectado y sus características (marca, modelo, versión de IOS, etc.), por lo que esta información puede ser obtenida aprovechándose de la actividad del protocolo CDP

en las interfaces que no son necesarias como aquellas conectadas a dispositivos finales (PCs, laptops, impresoras, etc.). Se considera un ataque de reconocimiento.

Para realizar la prueba de concepto se utilizó la herramienta Yersinia en modo interactivo. En la Fig. 3 se puede observar la información obtenida a partir del envío de mensajes CDP. La información obtenida en el ejercicio es de un equipo Catalyst 2960, de 24 puertos FastEthernet, que incluye datos sobre el IOS o sistema operativo del equipo. La valoración de la vulnerabilidad se muestra en la Tabla III.

Para mitigar el aprovechamiento del protocolo de descubrimiento se debe deshabilitar los anuncios de CDP en las interfaces que no están conectados a equipos de red.

Para deshabilitar en una interfaz específica:

```
S(config-if)#no cdp enable
```

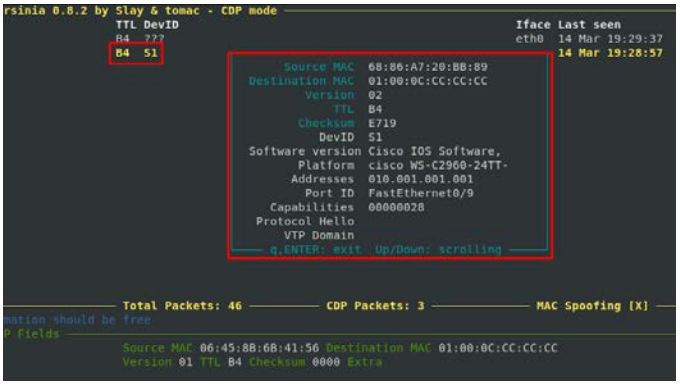

Fig. 3. Información obtenida de CDP

TABLA IV. VALORACIÓN CVSS DE APROVECHAMIENTO CDP

Métrica Base	Valor
Vector de ataque	Adyacente
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguno
Alcance	Sin cambios
Confidencialidad	Bajo
Integridad	Ninguno
Disponibilidad	Ninguno
Puntuación Base CVSS v3.0	**4.3**

La Tabla IV muestra el resultado de la valoración del nivel de severidad CVSS para la vulnerabilidad que permite el aprovechamiento CDP, el cual está establecido en 4.3, es decir un nivel medio, debido a que el vector de ataque es de modo adyacente, significa que se necesita estar en el mismo dominio de broadcast para que el ataque sea exitoso, además de solo afectar la confidencialidad de manera baja.

C. Prueba de concepto de ataque a DTP (Dynamic Trunk Protocol)

Para realizar la prueba de concepto para la explotación referida a VLAN en switches se ha establecido el escenario mostrado en la Fig. 4.

El Protocolo Troncal Dinámico (DTP por sus siglas en inglés) propietario de Cisco, tiene como función principal negociar un enlace para convertirse en un enlace troncal o no. Para tal efecto, las interfaces deben tener habilitado la negociación dinámica. La vulnerabilidad radica en que la negociación está habilitada por defecto en las interfaces que conectan dispositivos finales, por lo que esto puede ser aprovechado por atacantes para establecer un enlace troncal no deseado, consiguiendo de esta manera al tráfico de todas las VLANs permitidas en los enlaces troncales.

Para realizar la prueba de concepto se utilizó la herramienta Yersinia.

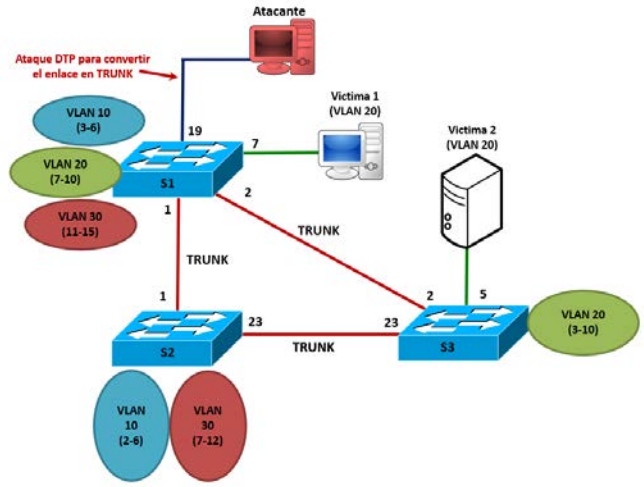

Fig. 4. Topología para Pruebas de Concepto de DTP

En la Fig. 5, se puede observar la negociación del protocolo DTP para lograr un enlace troncal con el equipo atacante.

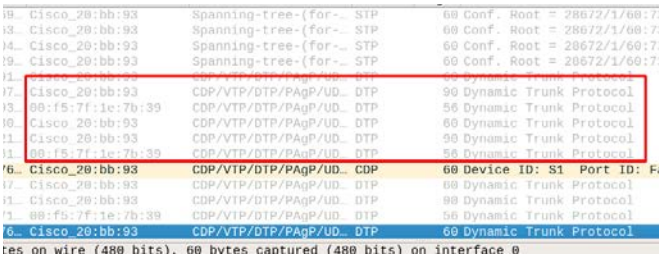

Fig. 5. Negociación DTP con Yersinia

Después de la negociación de enlace troncal, se puede verificar en el switch (S1) estableció un enlace troncal de forma automática. La Fig. 6 muestra la tabla de enlaces troncales en el switch S1, y la interfaz Fa0/19 se ha convertido en un enlace troncal, y esta interfaz es la que conecta a una PCs que es el equipo atacante.

```
S1#sh int trun

Port        Mode             Encapsulation  Status
Fa0/1       on               802.1q         trunking
Fa0/2       on               802.1q         trunking
Fa0/19      auto             802.1q         trunking

Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094
Fa0/19      1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30
Fa0/2       1,10,20,30
Fa0/19      1,10,20,30
```

Fig. 6. Enlaces Troncales en el switch S1.

Asimismo, se puede visualizar en la Fig. 7, el tráfico capturado que pertenece a otras VLANs, en este caso de la VLAN 10 (10.1.10.0/24).

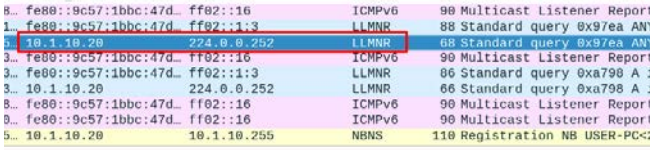

Fig. 7. Tráfico de otras VLAN capturado

La Tabla V muestra el resultado de la valoración del nivel de severidad CVSS para la vulnerabilidad que permite el ataque a DTP, el cual está establecido en 4.3, es decir un nivel medio, debido a que el vector de ataque es de modo adyacente, significa que se necesita estar en el mismo dominio de broadcast para que el ataque sea exitoso, además de solo afectar la confidencialidad de manera baja.

TABLA V. VALORACIÓN CVSS DE ATAQUE A DTP

Métrica Base	Valor
Vector de ataque	Adyacente
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguno
Alcance	Sin cambios
Confidencialidad	Bajo
Integridad	Ninguno
Disponibilidad	Ninguno
Puntuación Base CVSS v3.0	**4.3**

Para evitar la negociación de un enlace troncal en interfaces no deseadas, se debe suprimir la negociación en la interfaz específica, de la siguiente forma:

```
S(config-if)# switchport mode access | trunk
S(config-if)# switchport nonegotiate
```

D. *DHCP Spoofing*

La prueba de concepto para DHCP Spoofing requiere de un servidor legitimo en la red experimental construida para las pruebas anteriores. La Fig. 8 muestra el escenario utilizado para el tipo de ataque de suplantación de servidor DHCP.

La Fig. 9 y Fig. 10 muestran los resultados de la prueba, utilizando como herramienta el módulo de Metasploit Framework auxiliary/server/dhcp.

Los hosts de la red local que tienen habilitado la configuración de sus direcciones IP mediante DHCP, recibiendo los parámetros falsos del servidor DHCP Rogue.

La Tabla VI muestra el resultado de la valoración del nivel de severidad CVSS para la vulnerabilidad que permite el aprovechamiento CDP, el cual está establecido en 5.3, es decir un nivel medio, debido a que el vector de ataque es de modo adyacente, significa que se necesita estar en el mismo dominio de broadcast para que el ataque sea exitoso, además de afectar la confidencialidad y disponibilidad de manera baja.

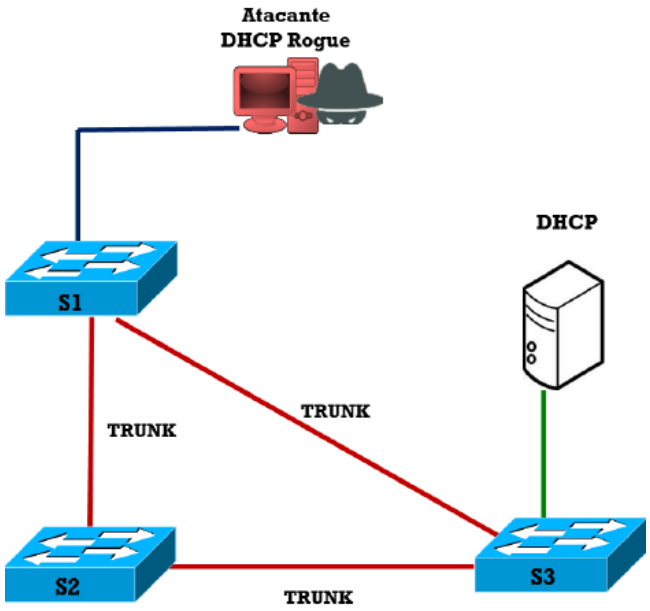

Fig. 8. Topología para Prueba de Concepto de DHCP Spoofing

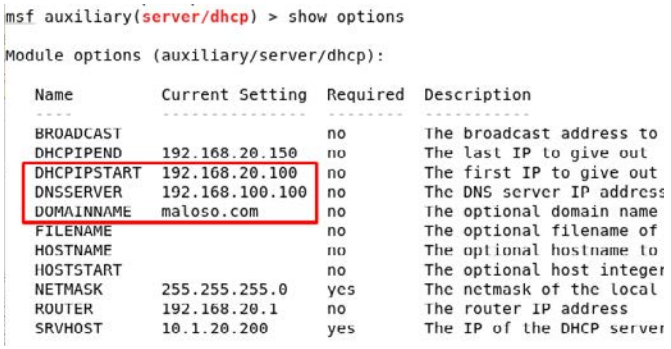

Fig. 9. Módulo de Mestasploit auxliary/server/dhcp

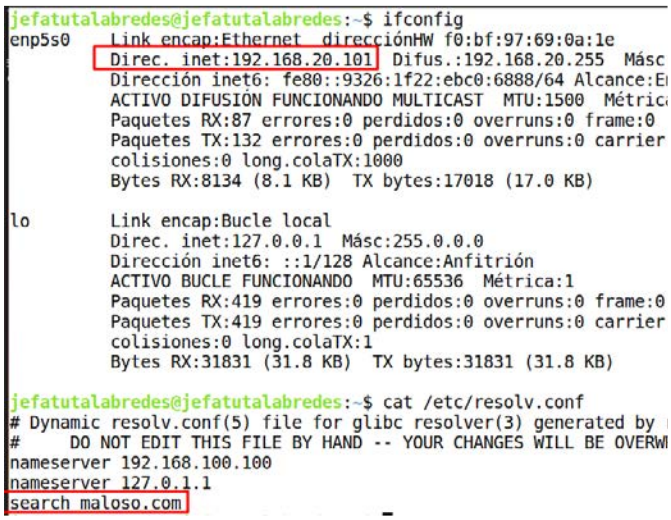

Fig. 10. Módulo de Mestasploit auxliary/server/dhcp

Para la mitigación se debe habilitar port-security y DHCP snooping en los switches para evitar el procesamiento y reenvío de mensajes DHCP (DHCPOFFER, DHCPDICOVER, DHCPREQUEST y DHCPACK) por los puertos de switch que no son de confianza; es decir por aquellos puertos donde no debería estar conectado un servidor DHCP.

TABLA VI. VALORACIÓN CVSS DE PRUEBA DE DCHP SPOOFING

Métrica Base	Valor
Vector de ataque	Adyacente
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguno
Alcance	Sin cambios
Confidencialidad	Bajo
Integridad	Ninguno
Disponibilidad	Bajo
Puntuación Base CVSS v3.0	**5.4**

E. ARP Poisoning – Main-in-the-middle

Un ataque de hombre en el medio a nivel de capa 2, requiere de un ataque previo como el de envenenamiento de ARP (ARP Poisoning) para que sea efectivo. La Fig. 11 muestra la topología utilizada para este tipo de prueba.

Las herramientas utilizadas para esta prueba fueron Ettercap para el envenenamiento de las tablas ARP de los hosts víctimas (ver Fig. 12) y el Wireshark para la verificación del ataque. La valoración de la vulnerabilidad se muestra en la Tabla VI.

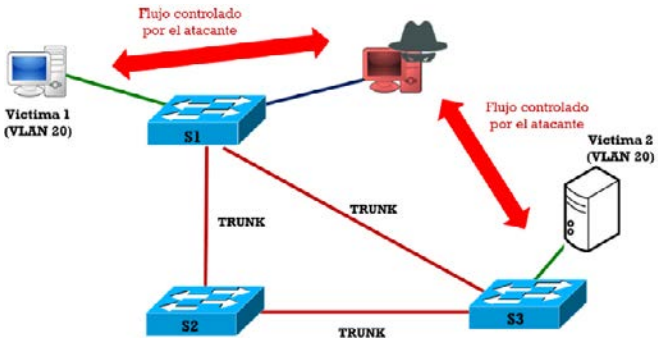

Fig. 11. Topología para la prueba de concepto de ARP Poisoning

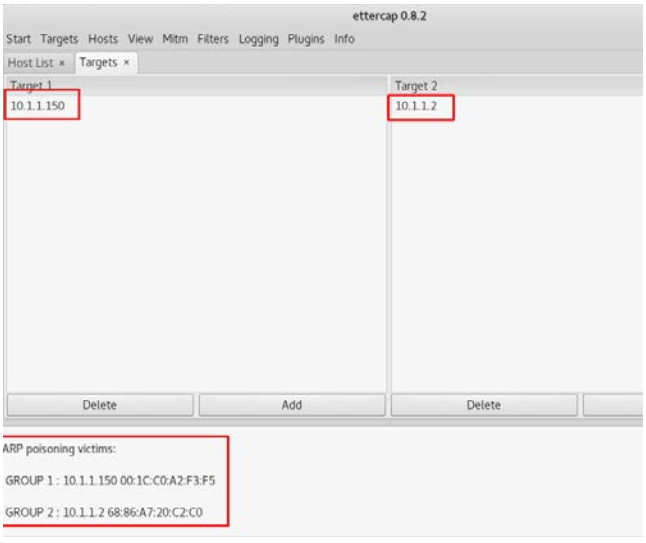

Fig. 12. Envenenamiento de ARP con Ettercap

TABLA VII. VALORACIÓN CVSS DE PRUEBA DE ARP SPOOFING

Métrica Base	Valor
Vector de ataque	Adyacente
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguno
Alcance	Sin cambios
Confidencialidad	Alto
Integridad	Ninguno
Disponibilidad	Ninguno
Puntuación Base CVSS v3.0	**6.5**

La Tabla VII muestra el resultado de la valoración del nivel de severidad CVSS para la vulnerabilidad que permite el al ataque de ARP Spoofing el cual está establecido en 6.5, es decir un nivel medio, debido a que el vector de ataque es de modo adyacente, significa que se necesita estar en el mismo dominio de broadcast para que el ataque sea exitoso, además de afectar la confidencialidad de forma alta, porque es posible la captura de mensajes eventualmente no cifrados que pueden contener información sensible o confidencial.

Para mitigar los ataques por envenenamiento de ARP, se debe habilitar el mecanismo de inspección dinámica de ARP en los puertos del switch

F. Ataque de diccionario Telnet y SSH

Para las pruebas de autenticación con protocolos de acceso remoto como TELNET y SSH, se realizaron ataques de diccionario. Como se muestra en la Fig. 13, los equipos admiten gran cantidad de intentos para autenticarse, lo que resulta una debilidad que puede ser aprovechada por agentes maliciosos al utilizar diccionarios que pueden ser elaborados de forma personalizada y ser exitosos al encontrar una credencial válida.

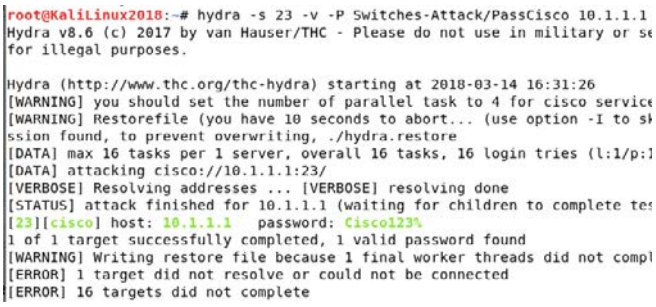

Fig. 13. Ataque de diccinario Telnet

La herramienta utilizada para esta prueba fue Hydra con un diccionario elaborado con palabras comunes que corresponden a contraseñas para este tipo de dispositivos.

La Tabla VIII muestra el resultado de la valoración del nivel de severidad CVSS para la vulnerabilidad que permite el ataque de diccionario contra servicios de Telnet y SSH, el cual está establecido en 5.3, es decir un nivel medio, debido a que el vector de ataque es a nivel de red, significa que es posible realizar el ataque de forma remota desde otros segmentos de red, además de afectar solo la confidencialidad de manera baja.

TABLA VIII. VALORACIÓN CVSS DE PRUEBA DE ATAQUE DE DICCIONARIO CONTRA SERVICIOS TELNET Y SSH

Métrica Base	Valor
Vector de ataque	Red
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguno
Alcance	Sin cambios
Confidencialidad	Bajo
Integridad	Ninguno
Disponibilidad	Ninguno
Puntuación Base CVSS v3.0	**5.3**

Para mitigar esta vulnerabilidad se recomienda limitar el origen de las conexiones con listas de control de acceso (ACL).

G. Alineación con los Controles CIS

De acuerdo con la rúbrica formulada, el estudiante deberá asociar las pruebas de concepto con los controles que correspondan a los 20 controles críticos publicado por el Center for Internet Security (CIS). Un ejemplo de esta correspondencia se puede apreciar en la Tabla IX, donde se observa que se alinean principalmente con dos sub-controles correspondientes al control 11 de CIS "Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores".

TABLA IX. ALINEACIÓN CON LOS CONTROLES DE CIS

Prueba de concepto	Sub Control	Descripción
Claim root role	11.1. Mantener configuraciones de seguridad estandarizadas en equipos de red	Mantenga configuración de seguridad estandarizadas y documentados para todos los equipos de red autorizados
Suplantación de servidor DHCP		
ARP Poisoning, *Man-in-the-middle*		
Aprovechamiento de CDP		
Salto de VLAN Aprovechamiento DTP		
Ataque de fuerza bruta	11.2. Documentar las reglas de configuración de tráfico	Todas las reglas de configuración que permiten que el tráfico fluya a través de dispositivos de red deben documentarse en un sistema de gestión de configuración con un fin de negocio específico para cada regla, el nombre de un individuo específico responsable de esa necesidad de negocio y una duración esperada de la necesidad

H. Rúbrica para el desarrollo del Laboratorio

La rúbrica formulada es la que se muestra en la Tabla X que abarca las fases del Laboratorio propuesto.

TABLA X. RÚBRICA PARA DESARROLLO DEL LABORATORIO

Criterio	Nivel
Identificación de vulnerabilidad (reconocimiento)	*(4) Excelente.* Identifica con éxito la vulnerabilidad con el apoyo de herramientas adecuadas o de forma manual con previa detección de la presencia de operación de protocolo y/o puerto asociado.
	(3) Satisfactorio Puede identificar la vulnerabilidad con el apoyo de herramientas adecuadas o de forma manual con previa detección de la presencia de operación de protocolo y/o puerto asociado.
	(2) Puede Mejorar Ocasionalmente puede identificar la vulnerabilidad con el apoyo de herramientas adecuadas o de forma manual con previa detección de la presencia de operación de protocolo y/o puerto asociado.
	(1) Inadecuado (necesita ayuda) Necesita asistencia para identificar la vulnerabilidad con uso de herramientas adecuadas o de forma manual con previa detección de la presencia de operación de protocolo y/o puerto asociado
Verificación de vulnerabilidad	*(4) Excelente.* Verifica con éxito la presencia de la vulnerabilidad con el apoyo de herramientas seleccionadas adecuadamente.
	(3) Satisfactorio Puede verificar la presencia de la vulnerabilidad con el apoyo de herramientas seleccionadas adecuadamente.
	(2) Puede Mejorar Ocasionalmente puede verificar la presencia de la vulnerabilidad con el apoyo de herramientas seleccionadas adecuadamente
	(1) Inadecuado (necesita ayuda) Necesita asistencia para verificar la presencia de la vulnerabilidad con el apoyo de herramientas seleccionadas adecuadamente
Valoración CVSS	*(4) Excelente.* Realiza con éxito la valoración de cada vulnerabilidad verificada con las métricas base de CVSS v3 y considerando las características de las pruebas de concepto.
	(3) Satisfactorio Puede realizar la valoración de cada vulnerabilidad verificada con las métricas base de CVSS v3 y considerando las características de las pruebas de concepto.
	(2) Puede Mejorar Ocasionalmente puede realizar la valoración de cada vulnerabilidad verificada con las métricas base de CVSS v3 y considerando las características de las pruebas de concepto.
	(1) Inadecuado (necesita ayuda) Necesita asistencia para realizar la valoración de cada vulnerabilidad verificada con las métricas base de CVSS v3 y considerando las características de las pruebas de concepto.
Mitigación de la vulnerabilidad	*(4) Excelente.* Identifica con éxito la solución para mitigación y describe correctamente el procedimiento de la aplicación de las recomendaciones técnicas asociadas a la solución de mitigación.
	(3) Satisfactorio Puede identificar la solución para mitigación y describe correctamente el procedimiento de la aplicación de las recomendaciones técnicas asociadas a la solución de mitigación.
	(2) Puede Mejorar Ocasionalmente identifica la solución para mitigación y describe el procedimiento de la aplicación de las recomendaciones técnicas asociadas a la solución de mitigación.
	(1) Inadecuado (necesita ayuda)

	Necesita asistencia para identificar la solución de mitigación y describir correctamente el procedimiento de la aplicación de las recomendaciones técnicas asociadas a la solución de mitigación.
Alineación con controles CIS	*(4) Excelente.* Establece con éxito la correspondencia entre la vulnerabilidad y algún control o controles de CIS.
	(3) Satisfactorio Puede establecer la correspondencia entre la vulnerabilidad y algún control o controles de CIS
	(2) Puede Mejorar Ocasionalmente establece la correspondencia entre la vulnerabilidad y algún control o controles de CIS
	(1) Inadecuado (necesita ayuda) Necesita asistencia para establecer la correspondencia entre la vulnerabilidad y algún control o controles de CIS

IV. Discusión

El Laboratorio propuesto es una forma efectiva de fortalecer y apoyar el proceso de enseñanza-aprendizaje de la seguridad de redes, específicamente en infraestructuras basadas en switches administrables.

Las pruebas de concepto seleccionadas y las vulnerabilidades comunes son básicas, que en entornos de red de producción maduros probablemente no estan presentes, sin embargo, son vulnerabilidades aún vigentes y vectores de ataques válidos, además de ser una fuente de aprendizaje importante para los estudiantes de carreras afines.

En trabajos futuros es posible ampliar las características de las pruebas de concepto utilizando equipos de diversos fabricantes y controles adicionales como los contemplados en la ISO/IEC 27001, PCI, entre otros, de tal forma que el estudiante tenga un panorama más completo de los aspectos técnicos y de gestión de la seguridad informática; asimismo es deseable pasar a niveles más sofisticados de pruebas de concepto como la manipulación de mecanismos de criptografía, o ataques de Denegación de Servicio (DoS).

Las herramientas utilizadas no son las únicas con las que se puede desarrollar los laboratorios, sin embargo, se recomienda analizar cómo opera cada herramienta que se pretenda usar. El estudiante puede elegir distintas herramientas a las establecidas para el laboratorio, lo que puede permitir desarrollar capacidades de análisis complementarias.

Las recomendaciones de mitigación o corrección de las vulnerabilidades pueden ser tomadas de las indicaciones de los fabricantes, pero también pueden ser propuestas por el estudiante mostrando su eficiencia. De esta manera se deja abierto a las posibilidades de generar soluciones diversas.

V. Conclusiones

El Laboratorio propuesto como una forma de soporte y apoyo al proceso de enseñanza-aprendizaje de la seguridad de redes a nivel universitario ofrece un paquete práctico que incluye las fases generales y comunes de un ataque (seguridad ofensiva), los procedimientos de mitigación (seguridad defensiva) y los controles de seguridad basados en una referencia válida como CIS (gestión de la seguridad informática). Este laboratorio, aunque limitado a un solo fabricante y tipo de control, es útil y motivador.

Agradecimientos

Al Laboratorio de Redes y Seguridad y a la Facultad de Ingeniería en Informática y Sistemas de la Universidad Nacional Agraria de la Selva.

Referencias

[1] M. A. Rahman y E. Al-Shaer, «A declarative approach for global network security configuration verification and evaluation,» de *12th IFIP/IEEE International Symposium on Integrated Network Management*, 2011.

[2] ISO/IEC, «ISO/IEC 27002 -Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información,» ISO, 2013.

[3] J. Cioara, D. Minutella y H. & Stevenson, Exam Prep CCNA 640-802., Indianapolis: Pearson Education, 2008.

[4] W. K. Alzubaidi, L. Cai y S. A. Alyawer, «A New Verification Method To Prevent Security Threads Of Unsolicited Message In Ip Over Ethernet Networks,» *International Journal of Computer Networks & Communications,* vol. 4, nº 6, pp. 21-31, 2012.

[5] The MITRE Corporation., «CVE - Common Vulnerabilities and Exposures,» 2019. [En línea]. Available: https://cve.mitre.org/. [Último acceso: noviembre 2018].

[6] O. Santos y J. & Stuppi, CCNA Security 210-260, Indianapolis: Pearson Education - CiscoPress, 2015.

[7] FIRST.org, Inc, «Common Vulnerability Scoring System v3.1: Specification Document,» 2019. [En línea]. Available: https://www.first.org/cvss/v3.1/specification-document. [Último acceso: enero 2019].

[8] Center for Internet Security, «Center for Internet Security,» 2019. [En línea]. Available: https://www.cisecurity.org. [Último acceso: Diciembre 2018].

[9] W. R. Marchand, E. Vega y J. Santillan, «Capture the Flag for Computer Security Learning,» de *IX Congreso Iberoamericano de Seguridad Informática y IV Taller Educativo TIBETS*, Buenos Aires, 2017.

[10] A. Bechtsoudis y N. Sklavos, «Aiming at Higher Network Security Through Extensive Penetration Tests,» *IEEE Latin America Transactions,* vol. 10, nº 3, pp. 1752-1756, 2012.

[11] D. Shmaryahu, «Constructing Plan Trees for Simulated Penetration Testing,» de *The 26th International Conference on Automated Planning and Scheduling*, London, 2016.

[12] A. Tewai y A. Kumar Misra, «Evaluation and Taxonomy of Penetration Testing,» *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 3, nº 8, pp. 5297 - 5302, 2015.

[13] Cisco System, CCNA Routing & Switching, California: Cisco Press, 2016.

[14] Y. Bhaiji, «Understanding, Preventing, and Defending Against Layer 2 Attacks,» 2009. [En línea]. Available: https://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf. [Último acceso: Octubre 2018].

[15] G. Weidman, Penetration Testing. A Hands-on Introduction to Hacking, San Francisco, California: Law, 2014.

[16] N. Jaswal, Mastering Metasploit, Birmingham, Mumbai: Packt Publishing, 2015.

[17] C. McNab, Network Security Assessment, San Francisco: O Relly Media, 2015.

[18] P. Gonzáles Pérez, Metasploit para pentester, Madrid: 0xWord, 2014.

[19] T. Kiravuo, M. Sarela y J. Manner, «A Survey of Ethernet LAN Security,» *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* vol. 15, nº 3, p. 1477–1491, 2013.

William-Rogelio Marchand-Niño, Ingeniero de Sistemas otorgado por la Universidad Nacional del Centro del Perú, con maestría en Dirección Estratégica de TI de la Universidad de Piura, con 18 años de experiencia académica en UNAS, UDH, UPLA. Desde el año 2004 es profesor asociado en la UNAS. Ha impartido más de 90 cursos de pregrado en diferentes universidades. Instructor CISCO por 12 años. Posee múltiples certificaciones de la Industria como PMP, ITIL Foundation, CCNA, MTA. Director del Centro de Tecnologías de Información y Comunicación de la Universidad Nacional Agraria de la Selva. Miembro Senior de la IEEE.

José Martin Santillan Ruiz, Ingeniero en Informática y Sistemas de la Universidad Nacional Agraria de la Selva. Profesor auxiliar en la UNAS, con mas de 7 años de experiencia en docencia. Miembro IEEE. Coordinador del área de Gestión de la Red Corporativa en el Centro de Tecnologías de la Información y Comunicación de la UNAS-Perú en el año 2016-2017.