Prácticas de Seguridad para el Laboratorio de Simulación de Telecomunicaciones

Carina Punina C. [1] Lizzette Yépez N. [2] Patricia Chávez B. [3]
Facultad de Ingeniería Eléctrica y Computación. [1]
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
cppunina@espol.edu.ec [1] leyepez@fiec.espol.edu.ec[2]
Profesor FIEC-ESPOL, pchavez@fiec.espol.edu.ec [3]

Resumen

En este trabajo se presentan prácticas de seguridad para el Laboratorio de Simulación de Telecomunicaciones; para su desarrollo fue necesario estudiar cinco ataques informáticos en los cuales la principal vulnerabilidad explotada esté relacionada con la incorrecta configuración de los dispositivos de red estos son: envenenamiento ARP, vulnerando el protocolo WPA, vulnerando el protocolo VTP, doble etiquetado de VLAN y desbordamiento de buffer, el proyecto se realizó utilizando enrutadores, enrutadores inalámbricos, conmutadores y computadoras disponibles en el Laboratorio de Simulación de Telecomunicaciones, con estos equipos diseñamos una topología idónea en la que se pueda llevar a cabo cada ataque mediante herramientas de software libre como ettercap, aircrack-ng, yersinia, scapy y metasploit, realizamos pruebas de rendimiento a la red y a los dispositivos antes, durante y después de cada ataque, luego de asegurarnos de que los ataques únicamente afectaban al desempeño de la red, diseñamos en cada caso un documento didáctico para estudiantes y profesores que detalla cada uno de los pasos de los ataques y su respectiva mitigación, además de encuestas cuyas preguntas miden el progreso de los estudiantes luego de aplicada la práctica.

Palabras Claves: *prácticas, ataques, mitigación, vulnerabilidad.*

Abstract

In this paper, are shown security practices for Telecommunications Simulation Lab, for its development was necessary to study five computer attacks in which the main exploited vulnerability is related to incorrect configuration of network devices these are: ARP poisoning, WPA attack, VTP attack, VLAN double tagging and buffer overflow, for the project we used routers, wireless routers, switches and computers available in the Simulation Lab Telecommunications, we design an appropriate topology in which be able to perform each attack with these devices with free software tools like ettercap, aircrack-ng, yersinia, scapy and metasploit, we test the network and the devices performance before, during and after each attack, then we probed the attacks only affect the network performance, we designed in each case an educational document for students and teachers with details and steps of the attacks and their respective mitigation, in addition although we designed surveys whose questions student progress measure and these are applied before and after the practices.

Keywords: *practices, attacks, mitigation, vulnerability.*

1. Introducción

Las redes de comunicación se han convertido en un medio de transmisión muy utilizado tanto a nivel corporativo como a nivel residencial, debido a su popularidad, se vuelve una necesidad la protección de la información transmitida.

El ambiente laboral se torna cada vez más competitivo por esta razón un profesional de TI debe estar preparado para administrar y asegurar los dispositivos de red a su cargo.

Actualmente la Facultad de Ingeniería Eléctrica y Computación cuenta con un laboratorio en el cual se imparten prácticas orientadas a que los estudiantes comprendan fácilmente el funcionamiento de los dispositivos, protocolos y tecnologías de redes de comunicación por lo que es oportuno complementarlas con herramientas y metodologías para asegurar la información que transmiten las redes, para lo cual es necesario realizar este conjunto de prácticas que permitan a los estudiantes obtener experiencia en el ámbito de la seguridad y lograr una visión amplia de las redes de comunicación que administrarán o diseñarán en su vida profesional, de esta manera se busca incentivar a los estudiantes a especializarse y expandir sus conocimientos, mejorando sus oportunidades laborales.

2. Ataques en las redes de datos

2.1. Vulnerabilidades en dispositivos de red

El término vulnerabilidad se refiere a las debilidades que podrían poner en riesgo la seguridad de un sistema informático, en los dispositivos de red encontramos vulnerabilidades de diseño, implementación y uso [1].

Las debilidades en el diseño de los protocolos usados para la comunicación y las políticas de seguridad deficientes son un ejemplo de las vulnerabilidades de diseño que afectan a los dispositivos de red y crean agujeros de seguridad en los mismos [1].

Las vulnerabilidades de implementación son los errores de programación, el descuido de los fabricantes, la existencia de puertas traseras y los virus informáticos [1].

Las vulnerabilidades de uso son las configuraciones deficientes de los dispositivos de red que carecen de seguridad y representan una amenaza potencial para la organización [1].

En el presente proyecto nos centraremos en el estudio de este tipo de vulnerabilidades, ya que es importante que los estudiantes adquieran una cultura de seguridad y comprendan los riesgos que conlleva una configuración incorrecta de los dispositivos de red.

2.2. Tipos de ataques

Los ataques a las redes de comunicación cada vez se incrementan y perfeccionan, para este proyecto estudiamos ataques relacionados con la falta de seguridad en las configuraciones de los dispositivos de red. Los tipos de ataques son: denegación de servicio, hombre en el medio, fuerza bruta y desbordamiento de buffer.

La denegación de servicio es un tipo de ataque que provoca la pérdida de acceso a un servicio o conjunto de ellos el mayor tiempo posible [2], [3].

Hombre en el medio es una técnica en la cual el atacante se coloca en el medio de una conexión haciendo las veces de servidor y cliente; de esta manera intercepta toda la información [4].

Fuerza bruta es un tipo de ataque en el cual se logra descubrir la clave de un sistema mediante la comparación con un conjunto de palabras, por ejemplo un diccionario [5].

Desbordamiento de buffer es un tipo de ataque en el cual se sobrepasa la longitud de memoria reservada para los parámetros de una llamada a procedimiento, con el fin de sobrescribir la dirección de retorno del contador de programa, ocasionando que solo busque parámetros de procedimientos que no son correctamente comprobados antes de ser utilizados [6].

2.3. Herramientas de ataque

Las herramientas para realizar ataques en la red permiten detectar y explotar las vulnerabilidades de los dispositivos finales e intermedios y son muy útiles para descubrir fallos a nivel de seguridad [7].

Las herramientas utilizadas para llevar a cabo las prácticas de seguridad fueron: ettercap, aircrack-ng, yersinia, scapy y metasploit.

Ettercap es una herramienta de software libre que permite interceptar el tráfico e inyectar datos en una conexión establecida además de filtrar la información sin perder la sincronización de la conexión [8].

Aircrack-ng es un conjunto de herramientas que sirven para el monitoreo y análisis de redes inalámbricas, además descifra claves WEP y WPA permitiendo el acceso ilícito a redes aparentemente seguras [9].

Yersinia es una herramienta de software libre que sirve para realizar auditoría informática y permite detectar la correcta configuración de seguridad en los dispositivos de red de capa dos del modelo TCP/IP [10].

Scapy es una herramienta que permite generar paquetes falsos UDP ó TCP para desestabilizar la red [11].

Metasploit es una herramienta que sirve para el desarrollo, prueba, mejora y penetración a

diversos sistemas, trabaja con una base de datos de códigos de explotación y vulnerabilidades [7].

2.4. Delitos informáticos en Ecuador

Los delitos informáticos en Ecuador están en aumento, en los primeros seis meses del año anterior la fiscalía general registró a nivel nacional 1.354 casos de delitos financieros, la mayor cantidad de denuncias se registran en las provincias de Pichincha 563, Guayas 275 y Santa Elena 131 [12].

En el ESET Security Report Latinoamérica 2012 la tasa de infección de Malware en nuestro país es del 77,88 % [13].

Los delitos informáticos son una realidad actual en nuestro medio por lo que la seguridad de la información es una obligación en todo sistema de comunicación, esto incrementa la demanda de profesionales capacitados en el área.

3. Mecanismos de Seguridad en la Red

La seguridad en las redes de datos ha tenido una evolución considerable debido a que las empresas que manejan información sensible se han visto en la obligación de implementar soluciones de seguridad que cumplan parámetros específicos. Entre los mecanismos de seguridad tenemos: determinación de la línea base, prevención de ataques en la red, detección de ataques en la red y recopilación de información [14], [15], [16], [17].

3.1. Determinación de la línea base

La línea base es una medición de todos los indicadores contemplados en el diseño de un red, y sirve para recopilar información del rendimiento de los dispositivos en condiciones normales, para así poder detectar un funcionamiento anormal en la red, los pasos para establecer una línea base son: determinar datos a recopilar, identificar dispositivos y puertos de interés; y determinar el tiempo adecuado para las pruebas.

Para seleccionar los datos a recopilar se debe analizar la funcionalidad de la red y determinar cuáles son los equipos fundamentales para el correcto desempeño de la red [15], [18].

Para identificar los dispositivos y puertos de interés; únicamente se debe escoger aquellos dispositivos y puntos de conexión más importantes para que la red funcione correctamente y luego se mide su rendimiento [18], [19].

El tiempo de duración de la línea base varía de acuerdo al tiempo del funcionamiento de la red, en todo caso se pueden realizar tendencias semanales o mensuales dependiendo del tamaño de la red [18].

3.2. Prevención de ataques en la red

La prevención de ataques es la acción de preparar a un sistema ante un posible riesgo y amenaza, un sistema seguro debe contar con tres propiedades estas son: integridad, confidencialidad y disponibilidad de la información [14].

La integridad garantiza que los recursos del sistema puedan ser modificados únicamente por la persona autorizada, por los mecanismos de seguridad tales como firma digital o cifrado de datos [14], [20].

La Confidencialidad es una propiedad en la cual los datos deben estar al alcance de las personas, entidades o mecanismos autorizados, de forma autorizada y solamente en momentos autorizados [14], [19].

La disponibilidad es la propiedad de los datos que permite obtener los mismos en el momento y forma adecuada cuando son requeridos por el usuario autorizado [14], [19].

Para la prevención de ataques en la red es importante realizar un análisis y control de riesgos, el análisis de riesgos es un estudio preliminar de todos los elementos que componen un sistema de información: activos, amenazas, vulnerabilidades, ataques e impactos. El control de riesgos es el proceso donde se toman decisiones en base al funcionamiento, efectividad y cumplimiento de las medidas de seguridad, para ello es útil el uso de los servicios de seguridad que garantizan la seguridad de los sistemas o la transferencia de datos, en la tabla 1 se muestra la relación entre los mecanismos y servicios de seguridad [14], [21].

Tabla 1. Relación entre servicios de seguridad y mecanismos de seguridad [19].

AMENAZA	SERVICIO DE SEGURIDAD	MECANISMO DE SEGURIDAD
Acceso no autorizado Denegación del servicio	Control de acceso	*Lista de control de acceso *Cortafuego
(Ataques pasivos)	Confidencialidad	*Cifrado *Rellenado de tráfico
Modificación no autorizada de la información	Integridad del mensaje	*Firma digital *Funciones hash y cifrado
Repudio del mensaje	No repudio	*Firma digital *Certificado
Enmascaramiento	Autentificación	*Firma digital *Certificado

3.3. Detección de ataques en las redes de datos

La detección de ataques es el proceso de identificación y respuesta ante las actividades ilícitas observadas contra uno o varios recursos de la red permite clasificar y priorizar los incidentes.

Existen diversas formas de realizar este tipo de detecciones, en la actualidad encontramos compañías que se dedican únicamente a la fabricación de equipos y software para el reconocimiento y mitigación de ataques en la red, así tenemos sistemas de detección y prevención de intrusos, sistemas de monitoreo, cortafuegos, entre otros.

3.4. Recopilación de información

Es un proceso en el cual se recolecta información para someterla a análisis e indicar los sistemas que se vieron afectados con la intrusión [16], [17].

El análisis forense es una ciencia moderna que sirve para recolectar información y reconstruir lo que ha sucedido tras un incidente de seguridad, no es una medida preventiva puesto que se utiliza cuando el ataque ya ha tenido efecto [16].

4. Prácticas de Seguridad para el Laboratorio de Simulación de Telecomunicaciones

Debido al aumento de la inseguridad a la que se ve expuesta la información en la actualidad, y a la importancia que adquieren los mecanismos de seguridad en la red es necesario el estudio básico de medidas preventivas que incentiven a los estudiantes a profundizar temas relacionados con la protección de la información transmitida.

En este proyecto hemos diseñado un conjunto de prácticas de seguridad en las cuales los estudiantes cumplen dos roles estos son atacantes y víctimas, de esta manera logramos que su experiencia sea la de una situación de riesgo real, donde tendrán que utilizar herramientas de software libre para explotar vulnerabilidades de los dispositivos de red y luego deben corregir dichas vulnerabilidades y mitigar el ataque realizado.

Las prácticas fueron diseñadas empleando enrutadores, enrutadores inalámbricos, conmutadores, y computadoras disponibles en el Laboratorio de Simulación de Telecomunicaciones, en la figura 1 se muestra la metodología utilizada para cada una de las prácticas.

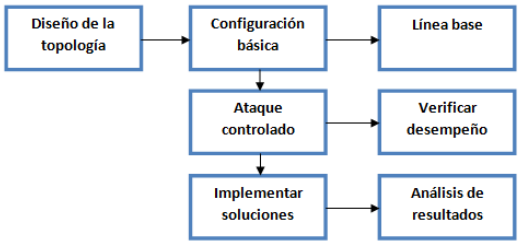

Figura 1. Diagrama básico de la metodología aplicada a las prácticas de seguridad

En cada práctica se diseñó una topología distinta que cumpla las condiciones óptimas necesarias para cada uno de los ataques, se estableció la línea base antes del ataque y después del mismo, con estas pruebas constatamos que ninguno de los ataques afectó el hardware de ningún equipo, y las únicas consecuencias se manifestaron en el desempeño y funcionamiento de la red.

Todas las prácticas fueron aplicadas a una muestra conformada por estudiantes de las carreras de Ingeniería en Telemática y Licenciatura en Redes y Sistemas Operativos, el proceso de realización de las prácticas fue el siguiente: inicialmente los estudiantes debían responder una encuesta que medía sus conocimientos previos, luego con un documento didáctico donde constan cada uno de los pasos para llevar a cabo el ataque, los estudiantes divididos en grupos y utilizando los dispositivos del laboratorio realizaron la práctica, la misma que contenía tres partes fundamentales: configuración, ataque y mitigación; finalmente los estudiantes debían responder una encuesta final en la cual calificaban la efectividad del documento proporcionado y contestaban preguntas dirigidas a medir los conocimientos adquiridos, todo esto con el objetivo de analizar el progreso del estudiante con este ejercicio.

4.1. Envenenamiento ARP

La topología utilizada para este ataque se muestra en la figura 2, y corresponde a un centro de compra y venta donde el conmutador del departamento de administración de la compañía no tenía seguridad en sus puertos y además conservaba algunas configuraciones predeterminadas por lo que cualquier dispositivo no autorizado podía conectarse y pertenecer a la

red, la máquina atacante se conectó al conmutador y en ésta se ejecutó la herramienta ettercap, mediante la cual nos colocamos en el medio de la conexión entre cliente y servidor, con el objetivo de obtener información sensible que se transmite entre ellos a través del envenenamiento de la tabla ARP de las computadoras del cliente y del servidor FTP.

La mitigación del ataque consiste en colocar configuraciones de seguridad al conmutador del departamento de administración, de manera que se apliquen restricciones a la cantidad de direcciones MAC y modos de violación del puerto, finalmente apagar los puertos que no están en uso en el conmutador.

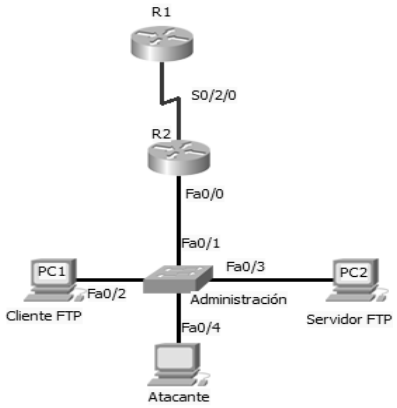

Figura 2. Topología envenenamiento ARP

4.2. Vulnerando el protocolo WPA

La topología utilizada para el ataque se muestra en la figura 3, y corresponde a un banco con dos departamentos, administración y gerencia además de una red inalámbrica para consultas de los clientes, en esta práctica se explotó la vulnerabilidad que presenta el protocolo WPA ante ataques de fuerza bruta cuando la clave de la red inalámbrica posee una seguridad débil, la herramienta usada fue aircrack-ng, adicionalmente el banco permitía la conexión de cualquier cliente inalámbrico a pesar de que sólo había una computadora autorizada para consultas.

La mitigación del ataque consiste en un conjunto de pasos entre ellos migrar al protocolo WPA2 aunque debemos tener en cuenta que esta migración no es efectiva, si no colocamos una clave segura, además se debe realizar un filtrado de MAC debido a que la única computadora autorizada para consultas es la de la sala de clientes.

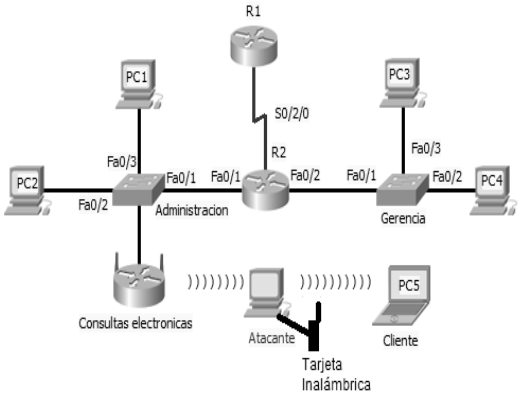

Figura 3. Topología envenenamiento ARP

4.3. Doble etiquetado de VLAN

En la práctica se enviaron tramas entre VLAN distintas sin que exista un dispositivo de capa tres que realice el cambio de etiqueta, la herramienta utilizada para realizar las tramas falsas fue scapy.

La topología mostrada en la figura 4 corresponde a un centro educativo cuyos conmutadores configurados de manera predeterminada tenían configurada como VLAN nativa una VLAN de datos, los puertos libres del conmutador tenían activa la negociación troncal.

La mitigación del ataque consistió en configurar los puertos libres en modo acceso y asignarlos a una VLAN distinta a la nativa y a la de datos, además se coloca seguridad en los puertos y se desactiva la negociación troncal en los puertos libres.

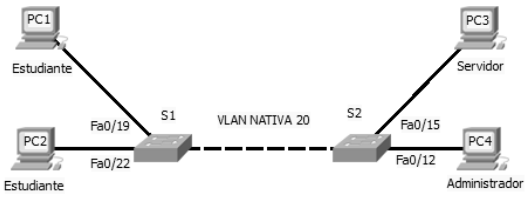

Figura 5. Topología doble etiquetado de VLAN

4.4. Vulnerando el protocolo VTP

En la práctica se explotaron las vulnerabilidades de los protocolos VTP y DTP, la herramienta usada fue yersinia.

La topología mostrada en la figura 6 correspondía a un centro de estudios, los conmutadores no tenían configuraciones de

seguridad y la negociación troncal se encontraba activa, por esta razón se pudo conectar una computadora que tenía instalada la herramienta y mediante envíos de paquetes DTP falsos se pudo ganar un enlace troncal por medio del cual la herramienta envía paquetes VTP indicando que la VLAN 10 ha sido borrada, esta actualización se transmite al servidor, luego al cliente y se crea una denegación de servicio entre las computadoras que pertenecen a VLAN 10.

Para mitigar este ataque colocamos los puertos en modo acceso, desactivamos la negociación troncal en los puertos de los conmutadores, aplicamos configuraciones de seguridad como limitar la cantidad de direcciones MAC y configurar el comportamiento del puerto ante una violación en la seguridad, crear una VLAN distinta y colocar en ella los puertos libres, una consideración importante es que si la red es muy pequeña y el protocolo VTP no es necesario, debe ser desactivado, caso contrario se debe colocar en la configuración del mismo una contraseña segura.

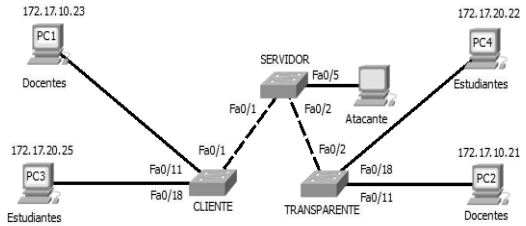

Figura 6. Topología vulnerando el protocolo VTP

4.5. Desbordamiento de buffer

En la práctica se realizó el ataque de desbordamiento de buffer explotando las vulnerabilidades del sistema operativo Microsoft Windows SP3/Profesional por medio de la herramienta metasploit.

La topología mostrada en la figura 7 correspondía a una inmobiliaria donde existían tres departamentos gerencia, recepción y el servidor de archivos, el enrutador utilizado en la red no tenía filtrada la comunicación entre los departamentos, por esta razón la recepcionista tenía acceso sin restricciones al servidor y al gerente, debido a que los dispositivos finales trabajaban con sistema operativo Windows XP SP3 se explotó la vulnerabilidad en el servicio SMB del puerto 445 denominada MSO9-067.

La mitigación del ataque consiste en configurar en el enrutador listas de control de acceso mediante las cuales limitamos la comunicación entre los departamentos y bloqueamos el tráfico generado desde la máquina atacante (recepcionista) hasta la máquina víctima (gerente) por el puerto 445 de TCP, finalmente protegimos los equipos finales con antivirus y cortafuegos.

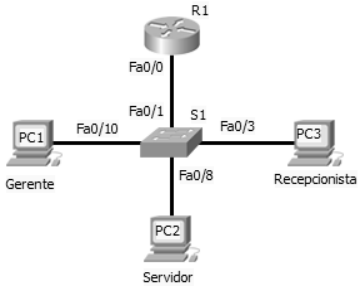

Figura 7. Topología desbordamiento de buffer

5. Análisis de resultados

El análisis de resultados está dividido en tres aspectos, progreso de los estudiantes que constituyeron la muestra, rendimiento de la red y rendimiento de equipos finales.

5.1. Progreso de los estudiantes

En la práctica de envenenamiento ARP la muestra estuvo constituida por quince estudiantes de la materia de conmutación y enrutamiento II (muestra A) y dieciséis estudiantes de la materia tecnologías WAN (muestra B). Los resultados se muestran en la tabla 2, donde se pueden observar los conocimientos adquiridos y el porcentaje de incremento de estudiantes que alcanzaron estos conocimientos luego de la práctica.

Tabla 2. Progreso de los estudiantes en la práctica envenenamiento ARP.

	PROGRESO	
CONOCIMIENTOS	**MUESTRA A**	**MUESTRA B**
Vulnerabilidades	33.32%	47.08%
Ataque envenenamiento ARP	26.67%	42.92%
Mitigación del envenenamiento ARP	52.66%	75%

En la práctica vulnerando el protocolo WPA la muestra estuvo constituida por veinte estudiantes de la materia conmutación y enrutamiento II (muestra C) y quince estudiantes

de la materia tecnologías WAN (muestra D). Los resultados se muestran en la tabla 3, se puede observar que la muestra tuvo un progreso mínimo esto se debe a que los estudiantes de dicha muestra tenían conocimientos avanzados del tema por lo que en términos de progreso no se puede evidenciar los porcentajes esperados.

Tabla 3. Progreso de los estudiantes en la práctica vulnerando el protocolo WPA.

	PROGRESO	
CONOCIMIENTOS	**MUESTRA C**	**MUESTRA D**
Vulnerabilidades	65%	4.33%
Elementos de una clave segura	35%	28%
Mitigación de la explotación al protocolo WPA	30%	0%

En la práctica de doble etiquetado de VLAN la muestra estuvo constituida por dieciocho estudiantes de la materia tecnologías de redes WAN (muestra E), en la tabla 4 se muestran los resultados del progreso de los estudiantes. Se puede evidenciar que el incremento del porcentaje de estudiantes en cuanto a la mitigación fue el máximo, esto refleja que ninguno de los miembros de la muestra tenía este conocimiento.

Tabla 4. Progreso de los estudiantes en la práctica doble etiquetado de VLAN.

	PROGRESO
CONOCIMIENTOS	**MUESTRA E**
Vulnerabilidades	16,66%
Ataque doble etiqueta	22.23%
Mitigación	100%

En la práctica vulnerando el protocolo VTP la muestra estuvo constituida por veintidós estudiantes de la materia tecnologías de redes WAN (muestra F), en la tabla 5 se muestran los resultados del progreso de los estudiantes.

Tabla 5. Progreso de los estudiantes en la práctica Vulnerando el protocolo VTP.

	PROGRESO
CONOCIMIENTOS	**MUESTRA F**
Vulnerabilidades	72.8%
Ataque VTP	27.32%
Mitigación	77.27%

En la práctica desbordamiento de buffer la muestra estuvo constituida por dieciocho estudiantes de la materia tecnologías de redes WAN (muestra E), los resultados del progreso de los estudiantes se muestran en la tabla 6, donde se demuestra la factibilidad de la práctica.

Tabla 6. Progreso de los estudiantes en la práctica desbordamiento de buffer.

	PROGRESO
CONOCIMIENTOS	**MUESTRA E**
Vulnerabilidades	78%
Ataque desbordamiento de buffer	89%
Mitigación	56%

5.2. Rendimiento de la red

En la práctica de envenenamiento ARP los tiempos de respuesta y la pérdida de paquetes se incrementaron en un 21.42% y 3.92% respectivamente, después del ataque el tiempo de respuesta tuvo una disminución del 50% y la pérdida de paquetes se incrementó en un 0.68 %, estos porcentajes han sido medidos con respecto a la línea base para ésta y todas las prácticas, podemos observar que el desempeño de la red se ve afectado, debido a que en este ataque se añade a la comunicación entre cliente y servidor FTP un dispositivo que incrementa la latencia de los paquetes.

En la práctica vulnerando el protocolo WPA el tiempo de respuesta se incrementó durante y después del ataque en un 8% y 5% respectivamente, la pérdida de paquetes tuvo una disminución durante y después del ataque del 25% y 50% respectivamente, con estos porcentajes podemos evidenciar que no se ve afectado el rendimiento de la red ya que la variación en el tiempo de respuesta es mínima con respecto a la línea base adicionalmente la pérdida de paquetes disminuye.

En la práctica doble etiquetado de VLAN la comunicación se ve afectada ya que los tiempos de respuesta y la pérdida de paquetes tuvieron un incremento del 40% y 0.11 % en la comunicación entre las computadoras de los estudiantes (ver figura 5), la comunicación entre el servidor y el administrador presenta un incremento del 20% en el tiempo de respuesta y del 0.30% en la pérdida de paquetes.

En la práctica vulnerando el protocolo VTP el tiempo de respuesta tuvo un incremento durante y después del ataque del 57% e infinito respectivamente, y la pérdida de paquetes disminuyó durante el ataque en un 0.35% y después del ataque se incrementó a un 100%, esto ocurre debido a que se realiza una denegación de servicio que impide la comunicación entre el

cliente y servidor FTP de la VLAN docentes que fue la atacada, ver figura 6.

En la práctica desbordamiento de buffer tenemos dos escenarios, en el primero se llevó a cabo el ataque con carga SHELL , donde la comunicación entre gerente, servidor y recepcionista (ver figura 7) se vieron afectadas, a continuación detallamos las variaciones de mayor prioridad, en la transferencia de archivos entre gerente y servidor hubo durante el ataque una pérdida de paquetes del 24,03% lo que disminuyó el tiempo de respuesta en un 27.28%, luego del ataque la pérdida de paquetes disminuyó en un 13.62% y el tiempo de respuesta se incrementó en 45.45% .

En la comunicación entre gerente y recepcionista el mayor cambio se observó luego del ataque donde la pérdida de paquetes se incrementó al 56.96%.

El escenario del ataque empleando la carga meterpreter provocó variaciones en la comunicación entre gerente, servidor y recepcionista (ver figura 7), las más importantes fueron: un aumento en el tiempo de respuesta del 100% en la comunicación entre gerente y servidor y en la transmisión de archivos una pérdida de paquetes del 23.43% todo esto durante el ataque , luego del ataque se presentó una disminución en la pérdida de paquetes del 14.07% con lo cual el tiempo de respuesta se incrementó en un 45.45%.

En la comunicación entre gerente y recepcionista luego del ataque se presenta un incremento en la pérdida de paquetes del 56.49% y una disminución en el tiempo de respuesta debido a la gran cantidad de paquetes perdidos del 16.67%.

5.3. Rendimiento de los dispositivos finales

En la práctica de envenenamiento ARP el cliente FTP presenta un aumento en el uso del procesador del 0.065% y en el uso de la memoria RAM una disminución del 0.1%, en el servidor FTP el incremento en el uso del procesador fue del 0.55% y en el caso de la memoria del 0.95%.

En la práctica vulnerando el protocolo WPA el cliente inalámbrico tuvo una disminución en el porcentaje de uso del procesador del 1.206% y el uso de la memoria RAM se incrementó en un 0.04%.

En la práctica doble etiquetado de VLAN el servidor y el administrador (ver figura 5) fueron las computadoras atacadas, en el servidor se incrementaron los porcentajes de uso del procesador y de la memoria RAM en un 2.81% y 0.88% respectivamente, y en el administrador el porcentaje de uso del procesador se redujo en un 19.8% y el porcentaje de uso de la memoria RAM se incrementó en un 0.60%

En la práctica vulnerando el protocolo VTP el cliente FTP presenta una disminución en el porcentaje de uso del procesador del 0.13% y un aumento en el porcentaje de uso de la memoria RAM del 0.1%, en el servidor FTP el porcentaje de uso del procesador disminuyó en un 0.3% y en el caso de la memoria aumentó en un 1.5%.

En la práctica desbordamiento de buffer la máquina del gerente presenta un aumento en el porcentaje de uso del procesador del 0.32% y una disminución en el uso de la memoria RAM del 0.3%.

5.4. Análisis final

Al realizar las encuestas podemos evidenciar que los estudiantes tienen progresos significativos con las prácticas realizadas, además también podemos observar que existe un mayor porcentaje de estudiantes que desconocen las vulnerabilidades de los dispositivos de red, a pesar de que este conocimiento básico es primordial en la formación de un futuro profesional del área de tecnologías de la información.

Al realizar las pruebas de rendimiento de la red podemos constatar que en algunos ataques como envenenamiento ARP , desbordamiento de buffer y vulnerando el protocolo VTP se ve afectado el desempeño de la red, debido a que el ataque en estudio provoca robo de información, denegación de servicio y control remoto de la máquina víctima respectivamente.

Los dispositivos intermedios como enrutadores y conmutadores no sufrieron cambios en su desempeño.

Con las pruebas de rendimiento a los dispositivos finales, se puede verificar que ninguno de los ataques afecta al hardware disponible en el laboratorio de simulación de telecomunicaciones, lo que incrementa la factibilidad de las prácticas de seguridad.

Los ataques seleccionados para las prácticas tienen las siguientes características comunes, en todos los casos las vulnerabilidades explotadas están relacionadas con el mal uso de los dispositivos de red por parte del administrador o la persona a cargo, las mitigaciones relacionadas con las configuraciones de seguridad básicas en los dispositivos de red son efectivas para cada uno de los ataques, el 75% de las practicas fue factible y mostró resultados que permitieron el análisis, la atención y las preguntas por parte de los estudiantes, de las cinco prácticas realizadas se

pudo observar que el envenenamiento ARP, vulnerando el protocolo WPA y el desbordamiento de buffer fueron las más aceptadas por los estudiantes, debido a que no existen demoras en la ejecución del ataque y los resultados que se observan son importantes tanto en el aprendizaje del estudiante y como material de apoyo de las clases regulares.

6. Conclusiones

1. En el presente trabajo se muestra la importancia de las prácticas de seguridad para los estudiantes de las carreras de Ingeniería en Telemática, Licenciatura en Redes y Sistemas Operativos quienes constituyeron la muestra para este estudio.
2. Se verifica que los estudiantes necesitan complementar sus clases regulares con prácticas de seguridad, debido al progreso que se evidenció en las encuestas posteriores a los laboratorios realizados.
3. Se demuestra que la práctica es un método efectivo de aprendizaje, y que los escenarios de riesgo donde el estudiante debe enfrentarse a problemas reales de seguridad contribuyeron en gran medida a la comprensión del tema.
4. Se comprueba que los documentos de soporte proporcionados a los estudiantes para llevar a cabo cada práctica son una herramienta didáctica con una estructura que permite su fácil lectura y comprensión.
5. Se demuestra que los ataques realizados en cada una de las prácticas no constituyen un riesgo para los dispositivos intermedios y los dispositivos finales, sin embargo afectan el correcto desempeño de la red.
6. Se demuestra que las prácticas con mayor factibilidad son Envenenamiento ARP y Desbordamiento de Buffer, debido a que los resultados obtenidos comprueban que su estructura, diseño, facilidad de comprensión y el poco tiempo empleado para su realización son favorables para complementar las clases regulares en el Laboratorio de Simulación de Telecomunicaciones.
7. Para lograr los objetivos planteados en cada práctica, éstas deben ser aplicadas a estudiantes que posean conocimientos básicos en redes de datos.
8. Las mitigaciones planteadas en cada una de las prácticas constituyen únicamente una forma de corregir los ataques, se debe incentivar al estudiante a investigar herramientas externas ya sea de software libre o licencias pagadas para aplicar seguridad a las redes y establecer comparaciones entre ellas. Todas las prácticas del presente trabajo fueron realizadas en IPV4 se recomienda en un estudio futuro trasladar los escenarios a IPV6.

7. Referencias

[1] Elvira Mifsud, “Introducción a la informática”, Monográfico, (2012), disponible:http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica, 8/01/2013,16h24.
[2] Arroyave Juan, Herrera J.,Vásquez E., "Propuesta de modelo para un Sistema Inteligente de Detección de Intrusos en Redes Informáticas (SIDIRI)", Escuela de Ingeniería de Antioquía, (2007), disponible : http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/ArtSidiri.pdf, 15/01/2013, 23h59.
[3] "Ataque por denegación de servicio", Kioskea.net, disponible: http://es.kioskea.net/contents/22-ataque-por-denegacion-de-servicio, 5/03/2013, 13h10.
[4] "El hombre en medio", Diario Informático, (2009), disponible: http://d3m0n1o.blogspot.com/2009/09/el-hombre-en-medio-es-un-tipo-de-ataque.html, 5/03/2013, 13h05.
[5] "Definición de fuerza bruta", Diccionario Informático, Alegsa, (2012), disponible : http://www.alegsa.com.ar/Dic/fuerza%20bruta.php, 18/05/2013, 10h00.
[6] Febrero Borja, Holguín J., "Pentest: Recolección de Información", INTECO, página 9.
[7] Zaragoza Jorge, "Manual básico Metasploit", disponible: http://www.paginasprodigy.com/jez2904/files/metasploit.pdf , 21/02/2013, 15h00.
[8] Urbina Julia ,Análisis y Evaluación de Sistemas para Detección de Intrusos en Redes de Computadoras, Universidad de las Américas Puebla, (2004), páginas 53,54.
[9] Aircrack-ng, (2013), disponible: http://www.aircrack-ng.org/doku.php, 21/02/2013, 20h30.
[10] Yersinia, Yersinia, disponible : http://www.yersinia.net, 6/03/2013, 16h04.
[11] Scapy, disponible en http://www.secdev.org/projects/scapy/doc/usage.html#interactive-tutorial, 6/03/2013, 21h00.
[12] "Promedio de siete delitos informáticos se registran por día", Radio Viva, (2012), disponible:

http://www.radioviva.com.ec/web/?p=6421 18/05/2013, 11h00.

[13] Eset Security Report Latinoamérica 2012, Laboratorios ESET,(2012), página 9, disponible: www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2012.pdf, 18/05/2013, 11h30.

[14] Chadwick D., Bertine H.,…Eucheder M., Vision General de asuntos relacionados con la Seguridad de las Telecomunicaciones y la Implementación UIT-T existentes, UIT, (2006), página 5.

[15] Farias M., Seguridad en el Router, (2008), disponible: http://seguridad.cudi.edu.mx/congresos/2008/cudi1/security.pdf.

[16] Rifa H., Serra J., Rivas J., Análisis Forense de Sistemas Informáticos, Eureca Media, Barcelona (2009), Primera Edición.

[17] García J. , Perramon X., Advanced aspect of Network Security, (2007), disponible: http://ocw.uoc.edu/computer-science-technology-and-ultimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01773.pdf , 19/11/2012, 9h00.

[18] Cisco System, Acceso a la WAN, (2008)

[19] Stalling W., Fundamentos de Seguridad en Redes Aplicaciones y Estándares, Prentice Hall, Madrid (2004), Segunda Edición.

[20] Aguilera Purificación, Seguridad Informática, Editex S.A W., Madrid (2010), Segunda Edición, 240 páginas.

[21] Junta Bancaria del Ecuador, Resolución No. JB-2011-1851, disponible: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2011/resol_JB-2011-1851.pdf, 11/12/2012, 10h00.