SEGURIDAD A TRAVES DEL PROTOCOLO DE RED IPV6 COMPARADO CON LA SEGURIDAD USANDO EL PROTOCOLO IPV4 PARA E-COMMERCE EN UNA INSTITUCION EDUCATIVA DE NIVEL SUPERIOR

Tec de Monterrey
CAMPUS MONTERREY

TESIS

MAESTRIA EN CIENCIAS EN TECNOLOGIA INFORMATICA

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS MONTERREY

Por:
ALEJANDRO SOLORIO CHAVEZ

DICIEMBRE DE 2001

SEGURIDAD A TRAVÉS DEL PROTOCOLO DE RED IPV6 COMPARADO CON LA SEGURIDAD USANDO EL PROTOCOLO IPV4 PARA E_COMMERCE EN UNA INSTITUCIÓN EDUCATIVA DE NIVEL SUPERIOR

Tec de Monterrey
CAMPUS MONTERREY

TESIS

MAESTRÍA EN CIENCIAS EN TECNOLOGÍA INFORMÁTICA

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

POR

ALEJANDRO SOLORIO CHÁVEZ

DICIEMBRE DE 2001

SEGURIDAD A TRAVÉS DEL PROTOCOLO DE RED IPV6 COMPARADO CON LA SEGURIDAD USANDO EL PROTOCOLO IPV4 PARA E_COMMERCE EN UNA INSTITUCIÓN EDUCATIVA DE NIVEL SUPERIOR

POR

ALEJANDRO SOLORIO CHÁVEZ

TESIS

Presentada a la División de Graduados en Electrónica, Computación, Información y Comunicaciones. Este trabajo es requisito parcial para obtener el Titulo de

Maestro en Ciencias en Tecnología Informática

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DICIEMBRE DE 2001

DEDICATORIA

A **Dios**, por darme el camino correcto para ser una persona de bien, por estar siempre conmigo.

A mis padres, **Juan y Enriqueta** por todo el apoyo y amor que me han dado, porque son parte muy importante de mi motivación de ser alguien importante y de provecho para este país.

A mis **hermanos** porque han estado en cada momento bueno o malo de mi vida, por siempre apoyar mis decisiones.

A mi hermano **Angel** y sobrino **Angel** por ser un motivo muy importante de mi superación profesional.

A mi amiga **Miriam Chan**, por apoyarme, por estar a mi lado en los tiempos buenos y malos del transcurso de mi maestría, y por ser una verdadera amiga.

A **Mirna Manjarrez Mora y Jorge Octavio Ávila Ramírez**, por la ayuda y confianza que siempre tuvieron en mi.

A **Angel Méndez**, por todo el apoyo que me ha brindado en los buenos y malos momentos, por ser mi mejor amigo.

A **Hector y Fernado**, por ser como una familia en Monterrey.

A **Jorge Orozco y Salvador Galván Infante**, por la ayuda que me brindaron y así poder estudiar mi maestría.

A **Marcela, Celina, Nayeli, Cristóbal, Mario, Carlos, Alfredo,** por todo el apoyo moral y su amistad incondicional.

A mis **amigos de Querétaro, Monterrey y Morelia**, por ser una parte importante en mi vida estudiantil.

A mis **amigos y compañeros de maestría**, por el apoyo y compañía en esta etapa de mi vida.

¡A todos ustedes muchas gracias!, Por contribuir a lograr este sueño tan importante para mí.

AGRADECIMIENTO

A mi asesor, **M. en C. Renán Rafael Silva Rubio**, por la guía y ayuda en el desarrollo del proyecto más importante hasta el momento de mi formación profesional.

A mis **sinodales M. en C. Raúl Ramírez Velarde y M. en C. Jaime Martínez Garza,** por el apoyo y las facilidades otorgadas en la terminación de esta tesis.

A **Miriam Chan Pavón**, por el apoyo técnico en el desarrollo de uno de los escenarios de la tesis.

A **Alfredo López Méndez**, por las facilidades al acceso del equipo para la implementación de los laboratorios y el apoyo técnico y moral otorgado.

A **Max Flores Pérez, Carlos Solano Rios, Cristóbal Castro Graff**, por el apoyo técnico y profesional otorgado para el desarrollo de la tesis.

A mis **maestros**, por compartir sus conocimientos y facilitar el desarrollo de la tesis.

Gracias a mi **familia** y **amigos**, por todo el apoyo moral.

A mis padres,
con cariño de
su hijo que
los quiere

RESUMEN

En esta tesis se evalúa y analiza la seguridad ofrecida al nivel de la capa de red por IPv6 contra las herramientas de seguridad implementadas en IPv4 para asegurar el e_commerce en una institución educativa. Esta evaluación y análisis se llevo a cabo mediante la implementación de cuatros escenarios que básicamente se resumen en IPv4 más mecanismos de seguridad (SET, SSL y VPN) e IPv6 implementando su seguridad, a los cuales se les aplico un análisis de riesgos y vulnerabilidades y pruebas de seguridad, en los que se baso para obtener los resultados y conclusiones de este trabajo de investigación.

TABLA DE CONTENIDO

DEDICATORIA ____ *iv*
AGRADECIMIENTO ____ *v*
RESUMEN ____ *vii*
LISTA DE FIGURAS ____ *xi*
LISTA DE TABLAS ____ *xiii*
CAPITULO 1 ____ *1*
INTRODUCCIÓN ____ *1*
1.1 HIPÓTESIS ____ **1**
1.2 OBJETIVO ____ **2**
1.3 JUSTIFICACIÓN ____ **2**
1.4 ALCANCES Y LIMITACIONES ____ **3**
1.5 RECURSOS ____ **4**
1.6 DESCRIPCIÓN DE LA TESIS ____ **5**
CAPITULO 2 ____ *7*
PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) Y SU SEGURIDAD ____ *7*
2.1 DESCRIPCIÓN DE IPV4 ____ **7**
2.2 DESVENTAJAS DE IPV4 ____ **9**
2.3 CAMBIOS DE IPV6 CON RESPECTO DE IPV4 ____ **9**
2.4 FORMATO GENERAL DE LA CABECERA IPV6 ____ **11**
2.4.1 FORMATO DE LA CABECERA IPV6 BASE. ____ 11
2.4.2 CABECERAS DE EXTENSIÓN DE IPV6 ____ 12
2.5 SEGURIDAD EN IPV6 ____ **13**
2.5.1 ASOCIACIÓN DE SEGURIDAD ____ 13
2.5.2 CABECERA DE AUTENTICACIÓN (AH) ____ 14
2.5.3 TÉCNICAS DE AUTENTICACIÓN ____ 15
2.5.4 ENCAPSULADO DE CARGA DE SEGURIDAD (ESP) ____ 16
2.5.5 TÉCNICAS DE ENCAPSULADO ____ 17
2.5.6 ADMINISTRACIÓN DE LLAVES ____ 18
2.5.6.1 ADMINISTRACIÓN MANUAL DE LLAVES ____ 18
2.5.6.2 ADMINISTRACIÓN DE LLAVES AUTOMÁTICA ____ 18
2.5.7 SEGURIDAD EN RUTEO ____ 19

CAPITULO 3 21

MECANISMOS DE SEGURIDAD EN E_COMMERCE 21

3.1 INTRODUCCIÓN 21

3.2 SEGURIDAD DE LA INFORMACIÓN 21

3.2.1 CRIPTOGRAFÍA 22

3.2.1.1 CRIPTOGRAFÍA SIMÉTRICA 22

3.2.1.2 CRIPTOGRAFÍA ASIMÉTRICA 23

3.2.2 PUBLIC KEY INFRASTRUCTURE (PKI) 24

3.2.3 CERTIFICADOS DIGITALES 24

3.3 SEGURIDAD EN ACCESOS 25

3.3.1 FIRMA DIGITAL 25

3.3.2 FIREWALLS 25

3.3.3 VIRTUAL PRIVATE NETWORK (VPN) 26

3.4 SEGURIDAD EN TRANSACCIONES 27

3.4.1 SECURE SOCKET LAYER (SSL) 27

3.4.2 SECURE ELECTRONIC TRANSACTION (SET) 28

3.5 SEGURIDAD EN SISTEMAS OPERATIVOS 29

3.5.1 UNIX 29

3.5.2 WINDOWS NT 30

3.6 SEGURIDAD EN CGI/API 30

3.7 SEGURIDAD EN LEGUAJES DE PROGRAMACIÓN 31

3.7.1 JAVA / JAVASCRIPT 31

3.7.1.1 JAVA 31

3.7.1.2 JAVASCRIPT 32

3.7.2 PERL 32

3.8 SEGURIDAD EN LA CONEXIÓN 33

3.9 HERRAMIENTAS DE MONITOREO 33

3.9.1 SNIFFERS 33

3.9.2 SCANNERS 34

3.9.3 DETECTORES DE INTRUSOS 34

CAPITULO 4 35

METODOLOGÍA 35

4.1 ESCENARIO 1: E_COMMERCE SOBRE IPv4 35

4.2 ESCENARIO 2: E_COMMERCE SOBRE IPv4 UTILIZANDO IBM SET DEMO 36

4.3 ESCENARIO 3: E_COMMERCE SOBRE IPv4 UTILIZANDO VPN 37

4.4 ESCENARIO 4: E_COMMERCE SOBRE IPv6 38

4.5 ANÁLISIS DE RIESGOS Y VULNERABILIDADES 41

CAPITULO 5 ____ *42*

RESULTADO DE LOS ANÁLISIS DE RIESGOS Y PRUEBAS DE SEGURIDAD EFECTUADOS EN IPv4 E IPv6 ____ *42*

5.1 ESCENARIO 1: E_COMMERCE SOBRE IPv4 ____ **42**
5.1.1 ANÁLISIS DE RIESGOS ____ 42
5.1.2 PRUEBAS DE SEGURIDAD ____ 44

5.2 ESCENARIO 2: E_COMMERCE SOBRE IPv4 UTILIZANDO IBM SET DEMO ____ **46**
5.2.1 ANÁLISIS DE RIESGOS ____ 46
5.2.2 PRUEBAS DE SEGURIDAD ____ 48

5.3 ESCENARIO 3: E_COMMERCE SOBRE IPv4 UTILIZANDO VPN ____ **49**
5.3.1 ANÁLISIS DE RIESGOS ____ 49
5.3.2 PRUEBAS DE SEGURIDAD ____ 52

5.4 ESCENARIO 4: E_COMMERCE SOBRE IPv6 ____ **54**
5.4.1 ANÁLISIS DE RIESGOS ____ 54
5.4.2 PRUEBAS DE SEGURIDAD ____ 55

CAPITULO 6 ____ *57*

CONCLUSIONES ____ *57*

6.1 CONCLUSIONES ____ **57**

6.2 TRABAJOS FUTUROS ____ **60**

ANEXO A ____ *61*

APLICACIÓN DESARROLLADA PARA SIMULAR E_COMMERCE ____ *61*

ANEXO B ____ *70*

FUNCIONAMIENTO DE IBM SET DEMO ____ *70*

ANEXO C ____ *75*

CONFIGURACIÓN DE LA VPN ____ *75*

ANEXO D ____ *79*

CONFIGURACIÓN DE SEGURIDAD EN IPv6 ____ *79*

ANEXO E ____ *87*

HERRAMIENTA DE DETECCIÓN DE RIESGOS Y VULNERABILIDADES Y HERRAMIENTA DE ATAQUE EXTERNO (SNIFFER) ____ *87*

REFERENCIAS BIBLIOGRÁFICAS ____ *97*

VITA ____ *100*

LISTA DE FIGURAS

FIGURA 2.1. FORMATO GENERAL DE LA CABECERA IPV4 7
FIGURA 2.2. MARCO DE TRANSMISIÓN DE INTERNET CON IPV6 11
FIGURA 2.3. FORMATO DE LA CABECERA IPV6 11
FIGURA 2.4. FORMATO DE LA CABECERA DE AUTENTICACIÓN 15
FIGURA 2.5. FORMATO DEL ENCAPSULADO DE CARGA DE SEGURIDAD 16
FIGURA 3.1. EJEMPLO DE CRIPTOGRAFÍA. 22
FIGURA 3.2. EJEMPLO DE CRIPTOGRAFÍA ASIMÉTRICA. 24
FIGURA 3.3. EJEMPLO DE FIREWALL SERVIDOR PROXY. 26
FIGURA 3.4. EJEMPLO DE ACCESO REMOTO Y VPN 27
FIGURA 3.5. EJEMPLO DE SSL. 28
FIGURA 3.6. EJEMPLO DE SET 28
FIGURA 3.7. EJEMPLO DE SNIFFER. 34
FIGURA 4.1 MODO TRANSPORTE IPV6/IPSEC 40
FIGURA 5.1 VULNERABILIDADES DEL ESCENARIO 1 AGRUPADAS POR NIVEL DE RIESGO 44
FIGURA 5.2 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 1 45
FIGURA 5.3 PANTALLA DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 1 VISUALIZANDO CUENTA Y PASSWORD 45
FIGURA 5.4 PANTALLA DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 1 VISUALIZANDO NÚMERO DE TARJETA DE CRÉDITO 46
FIGURA 5.5 VULNERABILIDADES DEL ESCENARIO 2 AGRUPADAS POR NIVEL DE RIESGO 47
FIGURA 5.6 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 2 48
FIGURA 5.7 PANTALLA DE UN PAQUETE DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 2 49
FIGURA 5.8 VULNERABILIDADES DEL ESCENARIO 3 AGRUPADAS POR NIVEL DE RIESGO 52
FIGURA 5.9 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 3 UTILIZANDO PPTP 53
FIGURA 5.10 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 3 UTILIZANDO L2TP 53
FIGURA 5.11 VULNERABILIDADES DEL ESCENARIO 4 AGRUPADAS POR NIVEL DE RIESGO 55
FIGURA 5.12 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 4 56
FIGURA A.1. PANTALLA DE ACCESO 62
FIGURA A.2. PANTALLA DE CURSOS DISPONIBLES 63
FIGURA A.3. PANTALLA DE CONFIRMACIÓN DE COMPRA. 63
FIGURA B.1 OBTENCIÓN DE IDENTIFICACIONES DIGITALES 72
FIGURA B.2 COMPRAR CON SET 73
FIGURA C.2.1 ESTATUS DE CONEXIÓN DE LA VPN 77
FIGURA C.2.2 DETALLES DE LA CONEXIÓN VPN UTILIZANDO EL PROTOCOLO PPTP 78
FIGURA C.2.3 DETALLES DE LA CONEXIÓN VPN UTILIZANDO EL PROTOCOLO L2TP 78
FIGURA E.1.1. EJEMPLO GRÁFICA 1 NETRECON 89
FIGURA E.1.2. EJEMPLO GRÁFICA 2 NETRECON 90

FIGURA E.1.3. EJEMPLO GRÁFICA 3 NETRECON 90
FIGURA E.1.4. EJEMPLO GRÁFICA 4 NETRECON 91
FIGURA E.2.1. PANTALLA PRINCIPAL DE ETHEREAL. 92
FIGURA E.2.2. EJEMPLO PANTALLA DE SALIDA DE ETHEREAL 93
FIGURA E.2.3. EJEMPLO PANTALLA DE SALIDA EN DETALLE DE ETHEREAL 94
FIGURA E.2.4. EJEMPLO PANTALLA DE SALIDA FOLLOW TCP STREAM DE ETHEREAL 95
FIGURA E.2.5. EJEMPLO DE FILTRO DE ETHEREAL 96

LISTA DE TABLAS

TABLA 2.1. CABECERAS DE EXTENSIÓN 12
TABLA 2.2. ORDEN DE LAS CABECERAS DE EXTENSIÓN 13
TABLA 4.1 CARACTERÍSTICAS DE CONFIGURACIÓN DEL MODO DE TRANSPORTE. 39
TABLA 5.1 VULNERABILIDADES ENCONTRADAS EN EL ESCENARIO 1 44
TABLA 5.2 VULNERABILIDADES ENCONTRADAS EN EL ESCENARIO 2 47
TABLA 5.3 VULNERABILIDADES DEL ESCENARIO 3 AGRUPADAS POR NIVEL DE RIESGO 52
TABLA 5.4 VULNERABILIDADES ENCONTRADAS EN EL ESCENARIO 4 55
TABLA 6.1 MECANISMOS DE SEGURIDAD IMPLEMENTADOS Y SU CAPA DEL MODELO TCP/IP U OSI 58
TABLA C.1.1 CARACTERÍSTICAS DEL SERVIDOR VPN 75
TABLA C.1.2. POLÍTICAS DE SEGURIDAD EN EL SERVIDOR VPN 76
TABLA D.1.1 CARACTERÍSTICAS DE LA CONFIGURACIÓN DEL HOST-A AL HOST-B 79
TABLA D.1.2 CARACTERÍSTICAS DE LA CONFIGURACIÓN DEL HOST-B AL HOST-A 80

CAPITULO 1

INTRODUCCIÓN

Con el desarrollo de Internet, paralelamente ha aparecido un nuevo concepto de Comercio, Comercio Electrónico.

Comercio Electrónico es hacer negocios de forma electrónica, donde un comprador de bienes o servicios utiliza un ordenador para interactuar con el ordenador del vendedor. Entre los negocios destacan, contratación electrónica de bienes y servicios, actividades tradicionales (banca, compras, etc) y nuevas (tiendas virtuales), para fin de esta tesis se enfocará al comercio electrónico en instituciones educativas.

Las comunicaciones atraviesan redes fuera del control de la organización origen y/o destino, pudiendo ser interceptadas, leídas, modificadas o, incluso, falsificadas. La necesidad de seguridad en el comercio electrónico es, por lo tanto, un problema crítico.

De ahí pues que se volvió necesaria la creación de mecanismos de seguridad estandarizados que asegurarán la interoperabilidad y proporcionen altos niveles de protección.

Actualmente el comercio electrónico en las instituciones educativas se lleva a cabo bajo el protocolo IPv4[1], el cual es complementado con mecanismos de seguridad, la finalidad de esta tesis es evaluar el nuevo protocolo de Internet IPv6[2], tratando de reducir la necesidad de mecanismos de seguridad y así poder reducir costos para las instituciones.

1.1 HIPÓTESIS

En un ambiente E_Commerce para una institución educativa de nivel superior la seguridad factible de implementar en redes usando el protocolo de Internet versión 6 (IPv6) es mayor que la seguridad posible de implementar en IPv4 con SSL, SET y VPN.

---

[1] IPv4: Protocolo de Internet versión 4

[2] IPv6: Protocolo de Internet versión 6

1.2 OBJETIVO

Evaluar y analizar la seguridad proporcionada por los protocolos de seguridad en IPv6 además de las herramientas de seguridad ofrecidas al mercado contra la seguridad implementada por IPv4 y herramientas de seguridad. Se espera que el nivel de seguridad proporcionado sobre IPv6 sea mayor debido principalmente al uso de protocolos de autenticación, encripción y manejo de encapsulado de carga de seguridad.

La comparación mencionada en la hipótesis se efectúa ante la expectativa de que la seguridad implementada con los protocolos en IPv6 pueda llegar a reducir la necesidad de utilizar herramientas de seguridad que a la fecha son usadas en IPv4 como SSL, SET y VPN.

Proporcionar un documento que sirva de guía de cómo implementar la seguridad en IPv6.

Contribuir con los esfuerzos realizados por la institución sobre investigación hecha en IPv6.

1.3 JUSTIFICACIÓN

El diseño original de Internet buscaba, entre otras cosas, la fiabilidad de las comunicaciones, de modo que la disponibilidad de un determinado enlace no afectara sensiblemente al conjunto de la red.

Las redes TCP/IP[3] basadas en IPv4 están plagadas con problemas de seguridad porque fueron diseñadas para trabajar en un ambiente amigable y con conexiones seguras. Cuando esta suposición no fue válida muchas debilidades de seguridad se manifestaron y fue fácil de explotar.

Generalmente, las comunicaciones atraviesan redes fuera del control de la organización origen y/o destino, pudiendo ser interceptadas, leídas, modificadas o, incluso, falsificadas. La necesidad de seguridad en este tipo de comunicación es, por lo tanto, un problema crítico.

De ahí pues que se volvió necesaria la creación de mecanismos de seguridad estandarizados que asegurarán la interoperabilidad y proporcionen altos niveles de protección.

[3] TCP/IP: Transfer Control Protocol / Internet Protocol

Para solventar las dificultades de seguridad en IPv4, las posibles soluciones son utilizar mecanismos de seguridad, como criptografía entre otros en el nivel aplicativo, para proteger los datos de transacciones electrónicas en el E_Commerce.

Actualmente, la introducción de mecanismos de seguridad en Internet se ha hecho cada vez más necesaria. Justamente, en la nueva versión de IP[4] (versión 6) se ha considerado obligatoria la implementación de estos mecanismos.

Considerando sus características de mejora en el desempeño de la red, incremento de la seguridad, y configuración automática de los nodos de la red, IPv6 se vislumbra como una opción clara para el sucesor de IPv4 dentro de algún tiempo. [BAY NETWORKS97] [IEEE NETWORK98]

1.4 ALCANCES Y LIMITACIONES

Se hizo una investigación teórica y practica. La investigación teórica se realizó en bibliografía disponible en el ITESM[5] y en Internet. La investigación practica se realizó en los laboratorios del sótano de CETEC[6] del ITESM, utilizando un modelo que se desarrolló para la simulación de la ejecución de transacciones.

Se desarrollo e implanto un sitio de E_Commerce para simular comercio electrónico, el cual tenía como función vender cursos a estudiantes de la universidad simulada y universidades que tenían convenio. Los pagos de los cursos eran por medio del pago de una tarjeta de crédito. Dicho sitio de E_Commerce se implanto sobre IPv4 e IPv6.

Se implementaron cuatro escenarios para comprobar la certeza o falsedad de la hipótesis. Los esquemas implementados fueron los siguientes:

1. IPv4 sobre plataforma Linux.
2. IPv4 incluyendo la herramienta de seguridad SET[7] y SSL[8], plataforma proporcionada por IBM[9].
3. IPv4 incluyendo las herramientas de seguridad VPN[10] sobre plataforma Windows 2000.
4. IPv6 con sus cabeceras de seguridad sobre plataforma FreeBSD.

[4] IP: Protocolo de Internet
[5] ITESM: Instituto Tecnológico y de Estudios Superiores de Monterrey
[6] CETEC: Centro de Tecnología Avanzada para la Producción
[7] SET: Secure Electronic Transaction
[8] SSL: Secure Socket Layer
[9] IBM: International Bussiness Machines, compañía de computadoras
[10] VPN: Virtual Private Network

El sitio de E_Commerce se implemento en 3 de los escenarios anteriores y en el segundo se utilizo un sitio de IBM, a los cuales se les hizo un análisis de riesgos y vulnerabilidades y un ataque externo para comprobar o rechazar la hipótesis.

Se realizaron entrevistas en las principales universidades de Monterrey para ver si ofrecen algún servicio de E_Commerce, en que consisten dichos servicios y con que mecanismos de seguridad garantizan la información. Dichas entrevistas tuvieron la finalidad de ver el esquema en que se encuentran y no se considera una muestra representativa.

1.5 RECURSOS

Se tuvo acceso al laboratorio ubicado en el sótano de CETEC del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey, en el cual se hicieron las pruebas e investigaciones sobre IPv4 e IPv6.

- *mainipv6.ipv6.com.mx*

  Características:

  Linux RedHat 6.1
  3ffe:1200:300a:2::9
  131.178.107.9
  Servidor web Apache (IPv4/IPv6)
  DNS, primario para ipv6.com.mx (IPv4/IPv6)

- *ipsec.ipv6.itesm.mx*

  Características:

  FreeBSD 4.4
  3ffe:8241::210:4bff:fe27:2048
  131.178.107.204
  Servidor Web Apache2 (IPv4/IPv6)

- *broker.ipv6.itesm.mx*

  Características:

  FreeBSD 4.4
  3ffe:8241::40

131.178.107.207
Servidor Web Apache2 (IPv4/IPv6)

- Laptop sin dominio

  Características:

  FreeBSD 4.4
  3ffe:8241::248:54ff:fec0:b87
  131.178.107.202
  Servidor Web Apache2 (IPv4/IPv6)

  Recurso al que se tuvo acceso en CETEC cuarto piso:

- medusa.mty.itesm.mx

  Características:

  Sistema Operativo Windows 2000 Server.
  IP: 131.178.21.42
  Computadora Intel Pentium III de 1 GHz.
  Disco duro de 30 GB.
  Memoria RAM de 256 MB.

Adicionalmente se utilizo la computadora portátil del tesista, la cual tiene las siguientes características:

- Laptop sin dominio

  Características:

  Windows 2000 Profesional
  Dirección dinámica
  Toshiba Satellite 1735
  Procesaro Intel Celeron a 700 Mhz.
  64 MB en Ram y 10 GB en disco duro.

1.6 DESCRIPCIÓN DE LA TESIS

El capítulo 2 hace una descripción general de IPv4, desventajas de este protocolo, cuales fueron los cambios hechos a este para crear IPv6 y finalmente

habla de la seguridad que implementa IPv6 por medio de sus cabeceras de extensión.

El capítulo 3 hace una descripción de los principales mecanismos de seguridad que se pueden implementar en IPv4 para complementar la seguridad.

El capítulo 4 hace una descripción de los escenarios implementados para corroborar o negar la hipótesis.

El capítulo 5 muestra los resultados obtenidos por la tesis basándose en los análisis hechos a los escenarios implementados.

El capítulo 6 muestra las conclusiones y los trabajos futuros propuestos.

Finalmente se tiene anexos para facilitar la lectura de la tesis, los cuales son sniffers utilizados, aplicación desarrollada para simular E_Commerce y configuración de los mecanismos de seguridad implementados.

CAPITULO 2

PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) Y SU SEGURIDAD

2.1 DESCRIPCIÓN DE IPV4

Las características principales del protocolo IP son que se trata de un protocolo no orientado a conexión y no fiable. Al ser no orientado a conexión, realiza la comunicación a través de paquetes, llamados datagramas. Al no existir conexión ni realizarse circuitos virtuales, los datagramas son tratados con encaminamiento individual. Esto significa que distintos datagramas procedentes de un mismo origen y con un mismo origen pueden llegar en desorden, duplicados o simplemente, perderse. Esto es lo que en arquitecturas de protocolos se entiende por protocolo no fiable. [Martín, 2000]

Se trata de un protocolo best effort(los hará lo mejor que pueda), lo que significa que, pese a que es admisible que descarte datagramas, no lo hará caprichosamente. [Martín, 2000]

El formato general de la cabecera IPv4 es el siguiente:

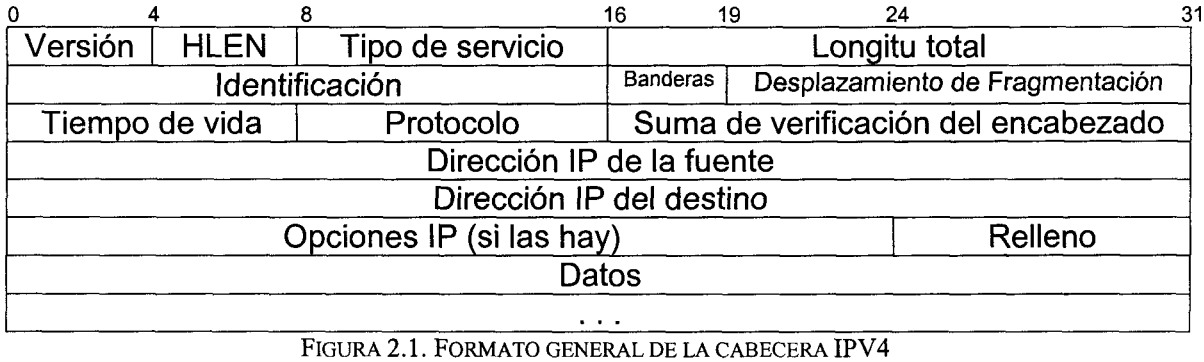


FIGURA 2.1. FORMATO GENERAL DE LA CABECERA IPV4

La figura 2.1 muestra el formato de un datagrama IPv4. Como es habitual en cualquier protocolo, consta de dos partes principales: una cabecera con información necesaria para el protocolo, y un cuerpo con los datos transportados.

La cabecera consta de una serie de campos obligatorios, lo que hace que su longitud mínima sea de 20 bits, y los otros opcionales. El significado y función de los mismo es el siguiente:

- *Versión*: 4 bits. Para IPv4 vale siempre 4 (como es obvio).
- *Longitud de la cabecera*: 4 bits. Como se ha dicho, la cabecera IPv4 tiene longitud variable, en función de los campos opcionales que utilice. Por ello se hace necesario este campo, con objeto de conocer dónde empieza el cuerpo de los datos.
- *Tipo de servicio*: 8 bits. Este campo es un intento (fallido) de diferenciar calidades de servicio. Está compuesto por un subcampo que indica la prioridad del datagrama y flags de un bit para indicar a los routers cuál es la preferencia del mismo si debe elegir entre retardo, caudal o fiabilidad. Sin embargo, desde las primeras implementaciones se ha hecho caso omiso de este campo, por lo que se puede afirmar que no tiene uso.
- *Longitud total del datagrama*: 16 bits. Indica la longitud en octetos de todo el datagrama, incluyendo la cabecera. Por tanto, la longitud máxima de un datagrama IPv4 será: 2^16= 64KB.
- *Campos de fragmentación*: 32 bits. *Identificación, Banderas* y *Desplazamiento de Fragmentación*, controlan la fragmentación y el reensamblado de los datagramas. El campo de *Identificación* contiene un entero único que identifica al datagrama. El campo *Desplazamiento de Fragmentación* especifica el desplazamiento en el datagrama original de los datos que se están acarreando en el fragmento. Los 2 bits de orden del campo *Banderas* controlan la fragmentación. El bit de orden inferior en el campo *Banderas* especifica si el fragmento contiene datos intermedios del datagrama origina o de la parte final.
- *TTL*: 8 bits. Tiempo de vida (Time To Live) del datagrama. Este campo expresaba en su definición original un tiempo de vida de los datagramas. Transcurrido éste, se descartaría. El objeto de esto sería defenderse ante bucles en el encaminamiento. En la práctica, se ha empleado como un contador decreciente de saltos, un valor que decrementará en una unidad en cada router que atraviesa el datagrama, con la misma finalidad. Un uso posterior que se le ha dado es limitar la distancia en saltos de las difusiones multicast.
- Protocolo: 8 bits. Indica a qué protocolo de nivel superior corresponden los datos transportados.
- Checksum de la cabecera: 16 bits. Contiene información redundante para comprobar la integridad de los datos de la cabecera.
- Dirección Origen: 32 bits. Dirección IPv4 del remitente del datagrama.
- Dirección Destino: 32 bits. Dirección IPv4 del destinatario último del datagrama.
- Campos Opcionales: a continuación de la parte fija de la cabecera y antes del cuerpo de datos, cabe la posibilidad de insertar campos opcionales

como encaminamiento en origen, registros de ruta (anotación de los nodos intermedios por los que pasa el datagrama) o timestamping (posibilidad de que cada nodo intermedio marque en el datagrama, la hora en que éste pasa por él).

2.2 DESVENTAJAS DE IPV4

El rápido crecimiento del Internet actual, el cual opera usando el protocolo de Internet versión 4 (IPv4; Internet Protocol version 4), ha creado un sinnúmero de problemas para la administración y operación de la red global. Estos problemas incluyen el decremento de direcciones IPv4 disponibles para nodos de red, la gestión de direcciones, la seguridad en las transferencias de información, el rápido crecimiento de los rendimientos de memoria y desempeño de los ruteadores, y la optimización de las comunicaciones multimedia.

Para dar solución a los problemas de IPv4, surge el protocolo de Internet de la siguiente generación: IPv6 (Internet Protocol version 6; Protocolo Internet versión 6).

2.3 CAMBIOS DE IPV6 CON RESPECTO DE IPV4

Entre los cambios de este protocolo respecto de IPv4, destacan los siguientes: [Bay Networks, 97] [IEEE Network, 98]

Expansión de las capacidades de direccionamiento: IPv6 incrementa el tamaño de las direcciones IP de 32 bits (IPv4) a 128 bits, para soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de autoconfiguración de direcciones. Esto garantiza rutas únicas para todas las variedades de red que se prevean para el futuro.

El direccionamiento es solamente uno de los muchos problemas que los diseñadores de IPv6 han abordado. Otras capacidades de IPv6 han sido desarrolladas en respuesta directa a los requerimientos críticos de negocio para arquitecturas de redes más escalables, como las mejoras en la seguridad e integridad de los datos, la calidad de servicio (QoS; Quality of Service) integrada a la autoconfiguración de direcciones, la computación móvil, y el multicasting de datos.

Simplificación de la cabecera: Algunos campos de la cabecera del IPv4 son eliminados o se hacen operaciones, tanto para reducir el costo de procesamiento como el tamaño de la cabecera.

Mayor flexibilidad para extensiones y nuevas opciones: En IPv6 no existe un campo de opciones como tal. La gestión de alternativas se realiza por un campo next header (siguiente cabecera), eliminando así las limitaciones de tamaño en la cabecera e introduciendo una gran flexibilidad en el desarrollo de nuevas opciones.

Autoconfiguración: Una de las características más notorias de IPv6 es su capacidad para configurar automáticamente un puesto con una dirección IP única, o bien de forma dinámica (similar a DHCP[11]). La configuración automática también concierne a las direcciones con el antiguo formato IPv4.

Esta nueva prestación reduce drásticamente la sobrecarga administrativa y la gestión de direcciones que caracterizaba hasta el momento al protocolo IP.

Capacidades de control de flujo: Se añaden a IPv6 nuevas capacidades que permiten marcar los paquetes que pertenezcan a un determinado tipo de tráfico, para el cual el remitente demanda una calidad mayor a la especificada por defecto o servicios en tiempo real.

Capacidades de autenticación y reserva de datos: IPv6 provee extensiones para soportar autenticación, integridad y confidencialidad de datos.

Soporte multimedia: IPv6 proporciona un soporte mejorado de aplicaciones multimedia y de tiempo real como la videoconferencia, la audioconferencia o las aplicaciones de control, gracias a la incorporación de dos nuevas características: las prioridades y las etiquetas de flujo.

La gestión de prioridades de los paquetes se realiza en función de la naturaleza de la información que transportan. Así, en el caso de una videoconferencia, el audio es considerado más importante que el video y, éste último, pero de baja definición, tendrá prioridad sobre el de alta definición.

Las etiquetas de flujo permiten a los paquetes entre dos direcciones específicas recibir una gestión particular por parte del RSVP (Resource Reservation Protocol; Protocolo de reserva de recursos), manteniendo una secuencia lógica de paquetes para garantizar el encaminamiento perfecto.

[11] DHCP: Dynamic Host Configuration Protocol

2.4 FORMATO GENERAL DE LA CABECERA IPV6

La cabecera IPv6 consiste de dos partes. Una es la cabecera IPv6 base, más las cabeceras de extensión opcional.

Encabezado Base	Extensión 1 de encabezado	. . .	Extensión N de encabezado	DATOS

FIGURA 2.2. MARCO DE TRANSMISIÓN DE INTERNET CON IPV6

2.4.1 FORMATO DE LA CABECERA IPV6 BASE.

0 – 4	4 – 12	12 – 16	16 – 24	24 – 31
Versión	Clase de Tráfico	Etiqueta de Flujo		
Longitud de carga útil		Siguiente cabecera	Limite de saltos	
Dirección de origen (16 bytes)				
Dirección de destino (16 bytes)				

FIGURA 2.3. FORMATO DE LA CABECERA IPV6

La cabecera del IPv6 tiene un tamaño fijo de 40 octetos, distribuido de la siguiente manera:

- Versión (4 bits): Número de versión; el valor actual es 6.
- Clase de Tráfico (8 bits): Identifica y distingue entre diferentes clases o prioridades de paquetes.
- Etiqueta de flujo (20 bits): Para aquellos paquetes que deben tener tratamiento especial por los encaminadores.
- Longitud de la carga útil (16 bits): Tamaño total de todas las cabeceras extendidas y los PDUs del nivel de transporte.
- Siguiente Cabecera (8 bits): Identifica el tipo de cabecera que está después de la cabecera IPv6.
- Límite de saltos (8 bits): El número permitido de saltos para el paquete. Esta es una simplificación del proceso llamado *time-to-live* del IPv4.

Decrementado de 1 en cada nodo que enviar adelante el paquete. El paquete es rechazado cuando este valor llega a cero.

- Dirección de origen (128 bits): La dirección del transmisor del paquete.
- Dirección de destino (128 bits): La dirección del receptor. Si la cabecera de encaminamiento está presente, posiblemente esta dirección no es del último receptor.

2.4.2 CABECERAS DE EXTENSIÓN DE IPV6

Las informaciones opcionales deben ser codificadas en cabeceras separadas entre la cabecera IPv6 y la cabecera del protocolo más arriba.

El procesamiento de estas cabeceras extendidas debe ser hecho estrictamente en la orden en que aparecen en el paquete y solo en el receptor. La única excepción es la cabecera salto-a-salto que debe ser examinada y procesada en todos los nodos a lo largo del camino. Su presencia es asignada a través del valor cero en el campo de "siguiente cabecera" de la cabecera de IPv6.

Si el campo de "siguiente cabecera" contiene un valor no reconocido por el nodo, entonces el paquete debe ser rechazado y un mensaje ICMP[12] de error debe ser encaminada al nodo transmisor.

Una especificación completa de IPv6 incluye las siguientes extensiones:

Cabecera de Extensión	Descripción
Opciones salto por salto	Información diversa para los enrutadores.
Enrutamiento	Ruta total o parcial a seguir.
Fragmentación	Manejo de fragmentos de datagramas.
Verificación de autenticidad	Comprobación de la identidad del transmisor.
Carga útil cifrada de seguridad	Información sobre el contenido cifrado.
Opciones de destino	Información adicional para el destino.

TABLA 2.1. CABECERAS DE EXTENSIÓN

Cuando más de una cabecera de extensión es utilizada, es recomendable que las cabeceras aparezcan en el siguiente orden:

[12] ICMP: Internet Control Message Protocol

Orden de las Cabeceras de Extensión
(1) Cabecera IPv6, obligatoria.
(2) Cabecera salto a salto.
(3) Cabecera de opciones de destino (ejecutado por el primer destino y por los otros después del primero).
(4) Cabecera encaminamiento.
(5) Cabecera fragmentación.
(6) Cabecera autenticación.
(7) Cabecera de encapsulado de seguridad de carga útil.
(8) Cabecera de opciones de destino (solo ejecutado por el último destino).

TABLA 2.2. ORDEN DE LAS CABECERAS DE EXTENSIÓN

Cada cabecera del IPv6 incluye un campo de "siguiente cabecera" que da de que tipo va a ser la próxima cabecera. También puede indicar el tipo de protocolo que está arriba de IPv6.

Cada cabecera de extensión debe ocurrir solo una vez con la excepción de la cabecera de Opciones de destino que ocurre dos veces.

Si la cabecera del nivel arriba es otra cabecera IPv6 (en los casos en que el IPv6 está encapsulado en IPv6) deben ser seguidas por sus respectivas cabeceras.

A pesar de la cabecera IPv6 sea mayor que la cabecera del IPv4, el IPv6 tiene menos campos. Por consiguiente, los encaminadores tendrán menos trabajo, aumentándose la eficiencia.

2.5 SEGURIDAD EN IPV6

Las especificaciones de IPv6 incluyen la descripción de dos cargas de seguridad: la *Cabecera de Autenticación* y el *Encapsulado de Carga de Seguridad*. Una provee autenticación, un procedimiento con el cual el receptor de un paquete puede garantizar que la dirección fuente es autentica y el que el paquete no ha sido alterado durante la transmisión. La otra garantiza que solo el receptor legítimo podrá leer el contenido del paquete. Ambas son basadas en un concepto de *Asociación de Seguridad*. [Huitema, 98]

2.5.1 ASOCIACIÓN DE SEGURIDAD

Autenticación y encripción requieren que el remitente y el receptor estén de acuerdo en una llave, en un algoritmo de autenticación o encripción, y en un

conjunto de parámetros auxiliares como el tiempo de vida de una llave o de la utilización de un algoritmo. Este conjunto de acuerdos constituye una Asociación de Seguridad entre los remitentes y los receptores. Cuando los paquetes son recibidos, solo pueden ser verificados o desencriptados si el receptor puede enlazarlos con el contexto de una Asociación de Seguridad. Todos los paquetes de autenticación y encripción transportan una *Índice de Parámetro de Seguridad (SPI)*. [Huitema, 98]

Cuando los paquetes son enviados a un único receptor a través de una dirección unicast, el SPI[13] es escogido por este receptor. Este debe ser, por ejemplo el índice dentro de una tabla de contenidos de seguridad mantenida por el receptor. El SPI a usar por cada socio de un host debe tener un parámetro de una Asociación de Seguridad. Cada estación debe recordar el SPI usado por su socio para identificar el contexto de seguridad. [Huitema, 98]

Cuando los paquetes son enviados a un grupo de receptores a través de una dirección multicast, el SPI es común para todos los miembros del grupo. [Huitema, 98]

El SPI es normalmente negociada como parte de un procedimiento de intercambio de llaves. [Huitema, 98]

2.5.2 CABECERA DE AUTENTICACIÓN (AH)

La Cabecera de Autenticación permite la integridad de datos y la autenticación de paquetes IP. Previene ataques de suplantación de direcciones. Impide ataques por sustitución. [Huitema, 98]

AH puede ser implementada en dos formas: modo de transporte (entre hosts) y modo túnel (entre hosts y puertas de seguridad). AH es un protocolo apropiado para implementar cuando la confidencialidad no es requerida, o no es permitida (quizás por regulaciones gubernamentales). [Miller, 2000]

La AH contiene los siguientes campos: [Morant, 2000]

- Cabecera Siguiente (8-bits): Identifica el tipo de la siguiente cabecera.
- Longitud de Carga (8-bits): Longitud de AH en palabras de 32-bits menos dos.
- Reserva (16 bits): Para uso futuro.
- Índice de Parámetros de Seguridad (32-bits): Identifica una AS[14].

[13] SPI: Índice de Parámetro de Seguridad
[14] AS: Asociación de Seguridad

- Número de Secuencia (32-bits): Contador.
- Datos de Autenticación: Debe ser un conjunto de palabras de 32 bits que contiene el Valor de Prueba de Integridad.

0	8	16 31
Cabecera Siguiente	Longitud de Carga	Reserva
Índice de Parámetros de Seguridad		
Número de Secuencia		
Datos de Autenticación		

FIGURA 2.4. FORMATO DE LA CABECERA DE AUTENTICACIÓN

2.5.3 TÉCNICAS DE AUTENTICACIÓN

El algoritmo sugerido en la arquitectura de seguridad de IP es conocido como *Keyed MD5*. Este es derivado del algoritmo Message Digest 5, MD5, diseñado por Ronald Rivest. MD5 calcula una suma de verificación de 128 bits del mensaje, o un código hash de 128 bits, usando transformaciones no lineales que hace una ingeniería inversa extremadamente difícil, aunque no enteramente imposible dando mucho tiempo y millones de dólares. Keyed MD5 opera combinando el mensaje con una llave secreta y después calcula el código hash en el resultado. [Huitema, 98]

El algoritmo para generar un Keyed MD5 es el siguiente: [Gai, 1998]

1. Dado un mensaje M a proteger, normalizarlo (M').
2. Rellenar el mensaje M' agregando tantos ceros bytes como sea necesario para alinear el mensaje como un múltiplo de 128 bits (mensaje M'_p).
3. Rellenar la llave K agregando tantos ceros bytes como sea necesario para alinear la llave como un múltiplo de 128 bits (mensaje K_p).
4. Calcular el valor de autenticación como un resultado de la función MD5 aplicando el argumento dado por la concatenación de K_p, M'_p, K_p.

El algoritmo de autenticación es negociado como parte de lo establecido en la asociación de seguridad. El algoritmo MD5 es especificado por default para asegurarse que todas las implementaciones pueden usar al menos un algoritmo común. Se puede esperar que otros algoritmos sean utilizados en el futuro – algoritmos que serán también rápidos de calcular o difíciles de crackear como MD5. [Huitema, 98]

605543

2.5.4 ENCAPSULADO DE CARGA DE SEGURIDAD (ESP)

La cabecera de autenticación no transforma los datos. Los datos permanecen limpios contra ataques de sniffers. Cuando la confidencialidad es deseada, la cabecera de *Encapsulado de Carga de Seguridad (ESP)* puede ser usada. [Huitema, 98]

La cabecera ESP esta diseñada para proporcionar confidencialidad, identificación de datos, integridad sin conexión, un servicio anti – respuesta, y confidencialidad limitada de flujo de tráfico. El servicio o servicios proporcionados depende de la Asociación de Seguridad y su implementación. [Miller, 2000]

El formato ESP es el siguiente:

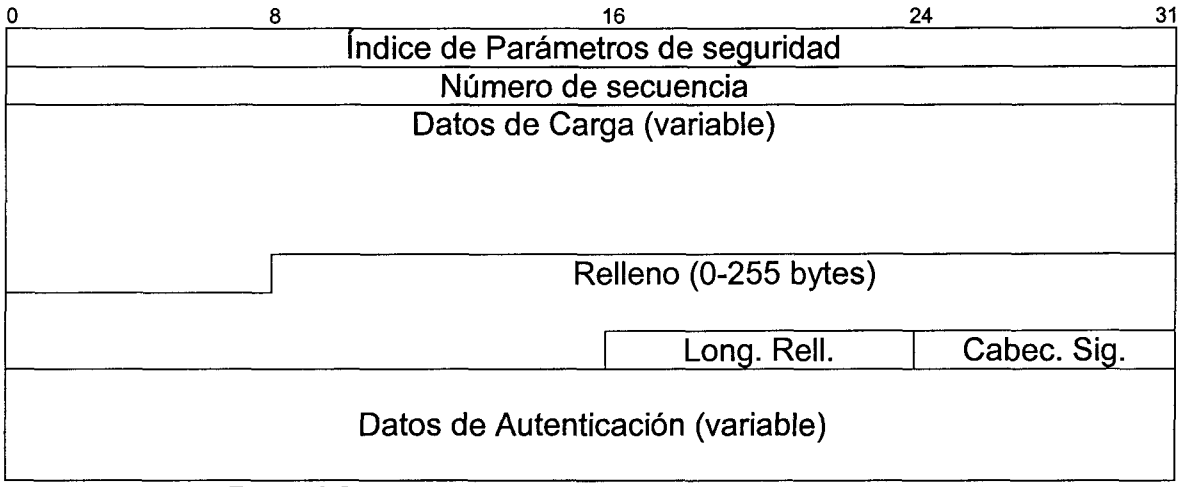


FIGURA 2.5. FORMATO DEL ENCAPSULADO DE CARGA DE SEGURIDAD

- Índice de Parámetros de Seguridad (SPI): 32bits que identifican una AS.
- Número de Secuencia: Un contador que proporciona una función antisustitución.
- Datos de Carga: En modo transporte es un segmento del nivel de transporte, y en modo túnel es un paquete IP cifrado.
- Relleno (0-255 bytes): Se expondrá después.
- Longitud de Relleno (8 bits): Indica el número de bytes del campo anterior.
- Cabecera Siguiente (8 bits): Identifica el tipo de contenido del campo Datos de Carga identificando la primera cabecera en dicho campo.
- Datos de Autenticación: Un campo de longitud variable cuya longitud es un número entero de palabras de 32 bits.

El campo de Relleno persigue varios objetivos:

- Si el algoritmo de cifrado necesita que texto en claro sea de una longitud determinada, éste campo permite conseguirlo.
- El formato ESP necesita que los campos Long. de Rell. y Cabec. Siguiente estén alineados a la derecha de una palabra de 32-bits. El campo Relleno se usa para conseguirlo.
- Se puede usar añadiendo algo de Relleno ocultando la longitud del campo Carga y posibilitando la confidencialidad de flujo de tráfico (parcial).

2.5.5 TÉCNICAS DE ENCAPSULADO

La técnica de encripción por default en IPv6 es DES[15]-CBC, donde el algoritmo DES es aplicado en modo Cipher Block Chaining (CBC). DES es un algoritmo de encripción de llave pública que es normalmente aplicado a bloques de 64 bits con una llave de 56 bits (extendida a 64 bits agregando un bit de paridad para cada 7 bits de la llave). Varias técnicas han sido propuestas para aplicar la transformación DES a bloques más grandes de 64 bits. El modo CBC divide la cadena de datos en una secuencia de bloques de 64 bits, y cada bloque se le aplica X-OR con el resultado de la encripción previa antes de que sea encriptada ella misma.

En el modo DES-CBC, la porción de encripción de la cabecera ESP comienza con un vector de inicialización (IV) compuesto de un número entero de palabras de 32 bit. En general, la longitud exacta del IV depende de cómo sea usada la Asociación de Seguridad.

El algoritmo DES-CBC debe estar disponible en todos los estándares de implementación de IPv6. Porque el algoritmo DES puede contemplarse como el mejor, moderadamente difícil de romper, es muy deseado que en un futuro cercano otros algoritmos sean estandarizados para usarse en IPv6. El algoritmo 3DES-CBC[16] es propuesto en el RFC[17] 1851. Está técnica esta basada en la repetición de la aplicación de la transformación DES al mismo bloque de datos con tres diferentes llaves, y es criptográficamente muy fuerte que el DES simple porque es equivalente a un algoritmo de encripción que usa una llave de 112 bits (en vez de una llave de 56 bits usada por DES). [Gai, 1998]

[15] DES: Data Encryption Standard
[16] 3DES: Triple Data Encryption Standard - Estándar de Triple Encriptación de Datos
[17] RFC: Request For Comments

2.5.6 ADMINISTRACIÓN DE LLAVES

La correcta aplicación de las cabeceras AH y ESP requiere que todas las partes de comunicación estén de acuerdo en una llave común que será usada en la formación y chequeo de las cabeceras de seguridad.

2.5.6.1 ADMINISTRACIÓN MANUAL DE LLAVES

IPv6 requiere que en cada implementación se permita la configuración manual de las llaves de seguridad, en el caso de la técnica de administración de llaves fuera de línea. Obviamente, la administración de llaves manual es posible sólo si los operadores de seguridad tienen un acuerdo en las llaves que serán usadas.

Esta solución tiene altos costos de personal y no es escalable porque requiere la acción personal de un operador en cada componente de la red tomando parte en el canal de seguridad. La intervención humana no asegura un alto nivel de seguridad, debido a operadores no confiables y problemas relacionados con la integridad del hardware y software del componente donde la llave será configurada.

La administración de llaves manual tiene aplicación en ambientes restringidos, con un número pequeño de componentes.

2.5.6.2 ADMINISTRACIÓN DE LLAVES AUTOMÁTICA

Administración de llaves es el área que menos ha sido establecida, la única decisión que se ha tomado, por generalidad, el protocolo de administración de llaves(IKMP, Internet Key Management Protocol – Protocolo de Administración de llaves de Internet) fue puesto en la capa de aplicación, y será independiente de los protocolos de las capas inferiores.

Una primera propuesta es basar IKMP en la pareja de protocolos ISAKMP y Oakley.

Internet Security Association and Key Management Protocol (ISAKMP Protocolo de Administración de Llaves y Asociación de Seguridad de Internet) define una arquitectura general para la configuración de autenticación

SA(asociación de seguridad) y el intercambio de llaves, sin la especificación de los algoritmos actuales a utilizar. De esta manera, esto puede ser utilizado con diferentes técnicas de intercambio de llaves.

Adicionalmente a la pareja ISAKMP – Oakley, diferentes soluciones ha sido propuestas. Actualmente, el mayor competidor es *Simple Key-management for Internet Protocols* (SKIP, Administración de Llaves Simple para Protocolos de Internet), que basa sus operaciones en el algoritmo de Diffie-Hellman. SKIP es simple y resuelve muchos problemas de administración de llaves en redes de alta velocidad, tal como actualización dinámica de llaves rápida (que es, cambio en línea frecuente de llaves de seguridad para evitar ataques analíticos basados en la acumulación de textos encriptados con la misma llave). SKIP no ha sido aun estandarizado.

Los diferentes protocolos de administración de llaves exhiben diferentes meritos que son valiosos en diferentes ambientes de aplicación.

2.5.7 SEGURIDAD EN RUTEO

Existen otras propiedades diferentes de seguridad disponibles a través de la combinación adecuada de las cabeceras de AH y ESP, es altamente deseable que estas sean aplicadas al intercambio de mensajes en los ruteadores para prevenir los ataques principalmente aquellos que dejan al descubierto la arquitectura lógica de la red.

Los tipos de comunicaciones que deben ser protegidos son los siguientes:

- El ruteo de mensajes de advertencias, para asegurar de que han sido originados por un ruteador autorizado.
- Los mensaje de advertencias de los vecinos para asegurar que viene de hosts asegurados y para prevenir el riesgo de que alguien agregue un nuevo host a la red sin previa autorización.
- El ICMP relativo a los host y redes inalcanzables (destino inalcanzable) o a mejores rutas (redireccionamiento), para asegurar que estos mensajes vienen de hosts o ruteadores que estaban en la ruta original de los paquetes.

La protección de las advertencias de los vecinos presenta un serio problema; estos mensajes pueden ser protegidos sólo después de que una asociación de seguridad ha sido creada entre el host y el centro de distribución de direcciones.

La protección contra falsos mensajes ICMP requiere que ellos sean protegidos por una cabecera AH, pero este enfoque tiene la desventaja de que requiere del establecimiento de una asociación de seguridad con cada ruteador y host en el camino entre la fuente y el destino de los paquetes.

Con respecto a la seguridad de los mensajes usados por varios de los protocolos de ruteo, ellos deberían siempre ser intercambiados sólo dentro del marco de una asociación de seguridad y deben ser protegidos por una cabecera AH.

Basado en el análisis anterior podemos concluir que la seguridad en ruteo es aparentemente un problema en IPv6, pero las probabilidades de resolver el problema son mucho mayores que IPv4.

CAPITULO 3

MECANISMOS DE SEGURIDAD EN E_COMMERCE

3.1 INTRODUCCIÓN

La seguridad es un principio básico en el e_commerce, un cliente requiere que su información personal no sea difundida a terceros y que sea empleada de manera inadecuada y sin autorización. Por el otro lado se encuentra el proveedor, que en este caso son las instituciones educativas, que su información crítica no sea compartida o interceptada y garantizárselo al cliente, queda más claro esto si ponemos como ejemplo, pago con tarjeta de crédito, el NIP, numero de tarjeta, nombre, no deben ser compartidos o interceptados.

La seguridad en el e_commerce no es simple, no basta con implementar un solo mecanismo de seguridad, requiere considerar muchos aspectos en diferentes niveles, para esto se requiere de varios mecanismos eficaces para garantizar la privacidad y la seguridad del sitio.

Este capítulo se enfocan a dar un panorama general de los mecanismos utilizados para mejorar la seguridad de un sitio de e_commerce.

3.2 SEGURIDAD DE LA INFORMACIÓN

Cuando se desea transmitir información entre computadores, especialmente a través de redes públicas, se plantea la necesidad de que la transmisión sea segura. La seguridad de la información transmitida tiene dos aspectos [Zamora]:

- *Que sea el destinatario del mensaje el único que pueda leerlo.*
- *Que nadie pueda suplantar la identidad del emisor del mensaje o modificar el contenido de los mensajes que envía.*

3.2.1 CRIPTOGRAFÍA

La criptografía es una técnica que permite la transformación de textos legibles en secuencias de caracteres no legibles. Esta técnica utiliza algoritmos y funciones matemáticas que permiten transformar la información en un conjunto de símbolos ilegibles y también permiten el proceso contrario. [Zamora]

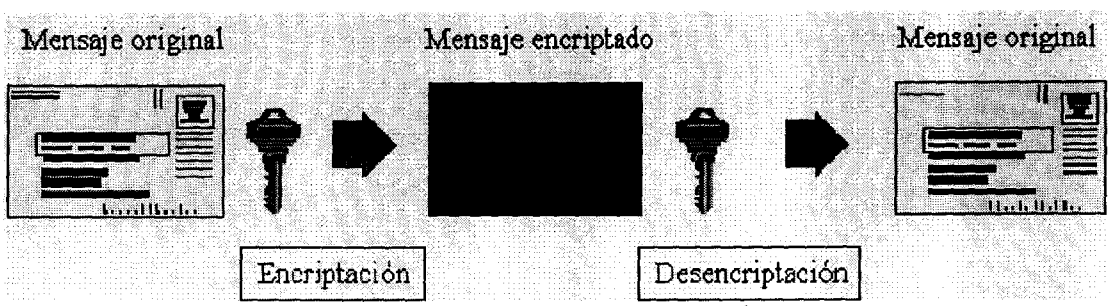


FIGURA 3.1. EJEMPLO DE CRIPTOGRAFÍA.

La criptografía se lleva a cabo mediante una transformación matemática y una llave. La llave contiene un código binario para la transformación matemática. Dos mecanismo de criptografía pueden ser usados para proporcionar la encripción: Criptografía Simétrica y Criptografía Asimétrica.

3.2.1.1 CRIPTOGRAFÍA SIMÉTRICA

Los algoritmos simétricos son algoritmos de llave privada donde la llave de desencripción es la misma que la de encripción. Estos son los algoritmos convencionales de criptografía donde el remitente y el destinatario deben de estar de acuerdo en la llave antes de que cualquier comunicación segura pueda llevarse a cabo entre ellos. Existen dos tipos de algoritmos simétricos los *algoritmos de bloques*, los cuales operan sobre el texto en claro en bloques de bits, y los *algoritmos de flujo*, los cuales operan en un bit único (o byte) del texto en claro a la vez. [Goralski, 99]

Los algoritmos simétricos pueden dividirse en dos categorías: *bloque y cadena*. Algoritmos de bloque encriptan los datos bloque por bloque, mientras que los algoritmos de cadena encriptan byte por byte. [Garfinkel, 1997]

Hay muchos algoritmos de llave simétrica usados en la actualidad. Algunos de los algoritmos que son comúnmente encontrados en el campo de la seguridad en Internet son resumidos en la siguiente lista [Garfinkel, 1997]:

- DES (Data Encryption Standard). Es un cifrador de bloques que usa una llave de 56 bits y tiene diferentes modos de operación dependiendo del propósito para el cual fue empleado. Tiene bloques de 64 bits.
- DESX. Es una modificación simple al algoritmo DES que es construido en dos pasos "blanqueados". Estos pasos aparecieron para mejorar la seguridad del algoritmo dramáticamente, efectivamente hace que la búsqueda de la llave sea imposible.
- Triple-DES. Es una forma de hacer que el algoritmo de DES sea al menos lo doble de seguro, usando el algoritmo de encripción DES tres veces con tres diferentes llaves.
- Blowfish. Es un algoritmo de encripción de bloque rápido, compacto y simple. El algoritmo permite una llave arriba de 448, y es optimizado por la ejecución de procesadores de 32 o 64 bits. El algoritmo ya no esta patentado y es de dominio público.
- IDEA (International Data Encryption Algorithm). Usa una llave de 128 bits y se cree que es poco fuerte.
- RC2, RC4. Es vendido con una implementación que usa una llave de entre 1 y 2048 bits. La llave es limitada a 40 bits en software que es vendido para exportación.
- RC5. Permite que el usuario defina el tamaño de la llave, el tamaño del bloque de datos, y el número de rondas de encripción.

3.2.1.2 CRIPTOGRAFÍA ASIMÉTRICA

Estos algoritmos direccionan el mayor inconveniente de los algoritmos simétricos, la necesidad de un canal seguro de intercambio de llaves. Este se basa en el uso de dos llaves diferentes: una llave pública la cual como su nombre lo implica, es conocida por todos, y una llave privada, la cual debe estar herméticamente segura por el poseedor. La llave privada no puede ser determinada por medio de la llave pública. El texto en claro encriptado con la llave pública solo puede ser desencriptado con la correspondiente llave privada, y viceversa. Un testo en claro encriptado con la llave privada solo puede ser desencriptada con la correspondiente llave pública. Así, si alguien envía un mensaje encriptado con la llave pública del destinatario, este puede ser leído solo por el destinatario al que fue enviado. [Goralski, 99]

Algunos de los algoritmos de Llave Asimétrica son [Silva, 2001]:

- Diffie y Hellman (1976, Universidad de Stanford)
- RSA (Rivest, Shamir, Adleman) basado en algunos principios de la teoría de números (productos de números primos y factores comunes)
- ELGAMAL basado en logaritmos discretos
- Merkle_Hellman basado en subconjuntos de sumatorias en combinaciones

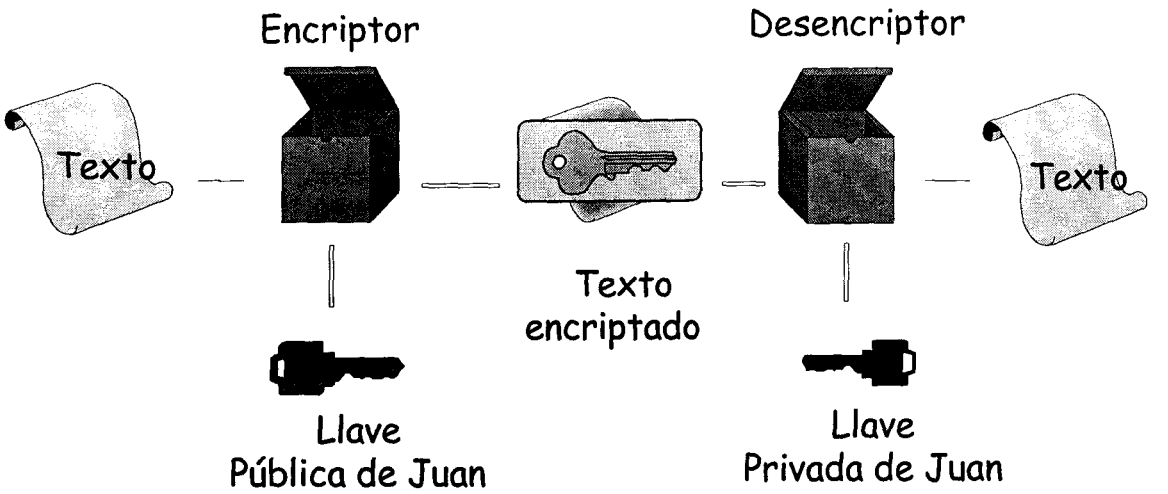


FIGURA 3.2. EJEMPLO DE CRIPTOGRAFÍA ASIMÉTRICA.

3.2.2 PUBLIC KEY INFRASTRUCTURE (PKI)

PKI son protocolos, servicios, y estándares que soportan aplicaciones de criptografía de llave pública. Incluye servicios y protocolos para manejo de llaves públicas, frecuentemente a través del uso de Certification Authority (CA) y Registration Authority (RA), no necesariamente efectúa operaciones de criptografía con las llaves.

Algunos servicios son:

- *Registro de llaves*: usando un certificado nuevo para una llave pública.
- *Revocación de certificados*: cancelando un certificado previamente emitido.
- *Selección de llave*: obteniendo una llave pública de un usuario
- *Evaluación de certeza*: determinando si un certificado es válido y que operaciones tiene autorizado.
- *Recuperación de llaves*. [Silva, 2001]

Se basan en el estándart de certificado X.509.

3.2.3 CERTIFICADOS DIGITALES

Son documentos digitales que atestiguan que una llave pública pertenece a una persona o entidad. Evita la impersonalización. Se usan para generar confidencia y legitimidad de una llave pública. En algunos casos se requiere crear cadenas de certificados donde cada certificado certifica al anterior. El certificado debe contener fecha de expiración, nombre de la autoridad certificadora que emitió

el certificado, un número de serie, etc. Contiene la firma digital del propietario de un certificado. Para certificar se usa el estándar ITU-T X.509 (International Telecommunications Union - Telecommunications standarization sector).

Los certificados son emitidos por una entidad certificadora (CA) con funciones notariales. [Silva, 2001]

3.3 SEGURIDAD EN ACCESOS

El control de acceso autentifica la identidad de la entidad (humano o computadora) tratando de accesar un recurso computacional, y controla el uso del recurso computacional predeterminando niveles de privilegio. [Rajput, 2000]

3.3.1 FIRMA DIGITAL

Garantizan que las partes implicadas en la transacción son quienes dicen ser y que los mensajes u ordenes de compra han sido recibidas tal y como fueron emitidas. Estas firmas se basan también en la criptografía y en la existencia y actuación de las *Autoridades Certificadoras* .

Es un tipo especial de encriptación. Más arriba se ha visto cómo se codifica un texto. Supóngase por un momento que se quiere garantizar la autenticidad, aunque no importe que alguien pueda leer el contenido del mensaje enviado, pero se quiere asegurar que el texto no es modificado después del envío. Para este fin se utiliza una combinación de un digest y la encriptación con clave pública. La firma digital consiste en añadir al mensaje, un digest encriptado del mensaje original; basta que alguien añada o cambie una sola letra, para que el digest del texto, no coincida con el digest encriptado del mensaje original. [Zamora]

3.3.2 FIREWALLS

Los Firewalls son una combinación de varios componentes – tal como routers, computadoras, y servidores proxy – que controlan el acceso redes internas. Algunas ventajas de los vendedores de nuevos firewalls es que proporcionan todos estos componentes en una sola plataforma. Los firewalls restringen a los usuarios de accesos a redes de corporaciones y limitan a los usuarios autorizados a accesar a ciertas aplicaciones y datos. Las ACLs (listas de control de acceso) y reglas de seguridad permiten la definición de tales reglas.

Los firewalls son filtros principalmente que examinan el contenido de los paquetes y rutean o rechazan la ruta de los paquetes basándose en su contenido. Firewalls implementa políticas de control de acceso entre dos redes. Los tipos básicos de firewalls son *filtros basados en paquetes.* Estos firewalls examinan las cabeceras de la dirección IP fuente o destino, y basado en las reglas de acceso rechaza o acepta la solicitud de conexión. Estos firewalls trabajan de manera simple analizando la dirección IP individualmente y no proporcionan análisis de las sesiones de red. El IP spoofing es el principal problema de estos firewalls.

Puertas de Aplicación son servidores proxy que corren en computadoras que actúan como un firewall. Servidores proxy son software de aplicación que actúan como servidor para las aplicaciones que solicitan conexión de la red protegida y actúan como clientes de los servidores. Esta característica del proxy en el firewall permite actuar al firewall como intermediario entre la solicitud del cliente en el nivel aplicativo, transporte o red. Aplicaciones de proxy completas auditan y filtran todo el trafico que va sobre ellas. [Rajput, 2000]

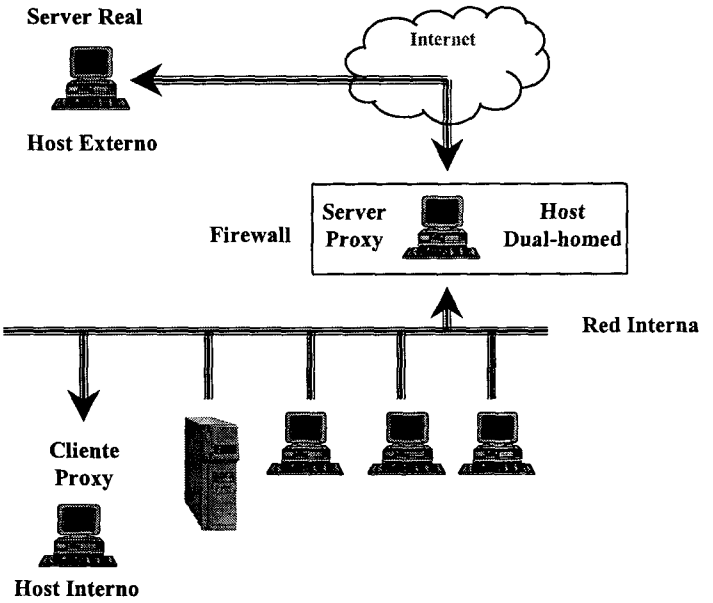


FIGURA 3.3. EJEMPLO DE FIREWALL SERVIDOR PROXY.

3.3.3 VIRTUAL PRIVATE NETWORK (VPN)

VPNs se refiere a túneles de datos seguros entre dos puntos sobre una red de datos pública y privada. El uso de VPNs requiere protocolos de software especial que asegure la confidencialidad e integridad de los datos sobre una red insegura entre dos puntos finales de una red.

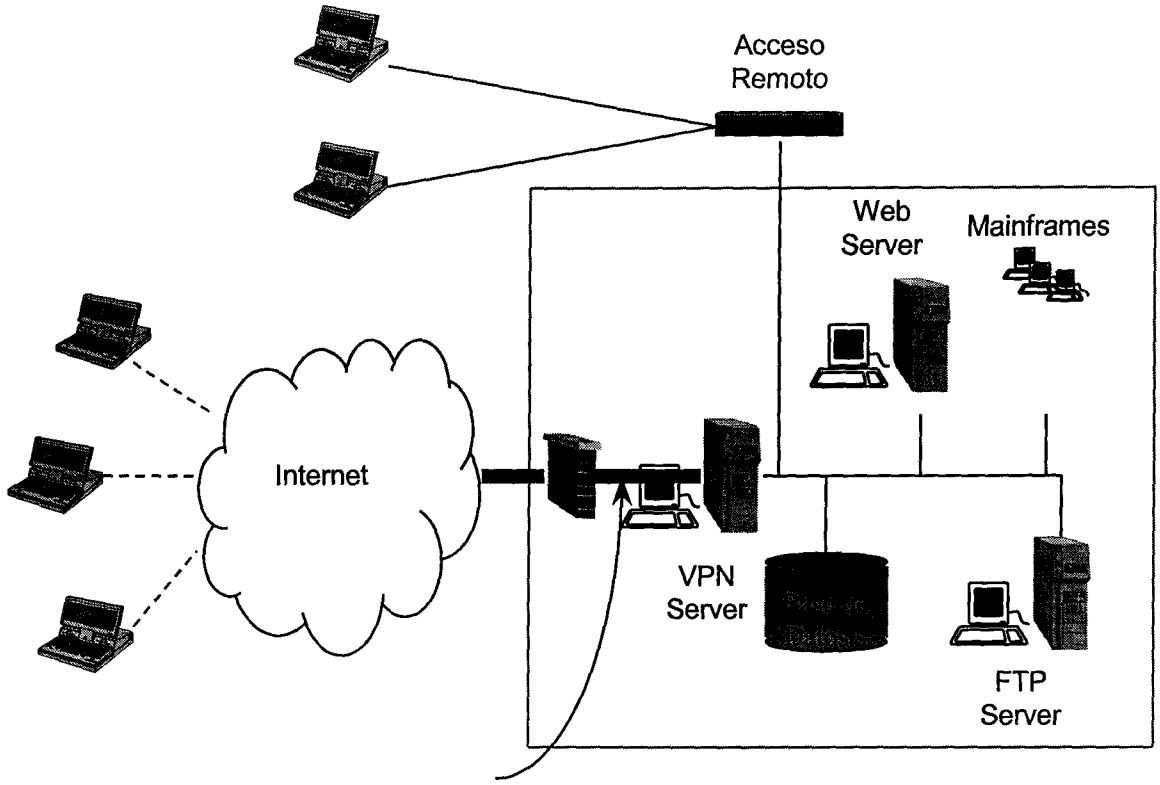


FIGURA 3.4. EJEMPLO DE ACCESO REMOTO Y VPN

3.4 SEGURIDAD EN TRANSACCIONES

La seguridad de las transacciones debe dar confianza a los clientes de que sus transacciones son seguras en Internet. Las transacciones seguras y el proceso de pago seguro es lo más importante para permitir el e_commerce. [Cameron, 1999]

3.4.1 SECURE SOCKET LAYER (SSL)

Netscape desarrollo el protocolo SSL para asegurar aplicaciones en Internet. SSL es independiente de la aplicación y puede asegurar las aplicaciones más populares de Internet (http, Telnet, FTP). El protocolo SSL incluye la autenticación del servidor y el cliente y proporciona un túnel en la capa de transporte para proporcionar confidencialidad de los datos entre dos aplicaciones en Internet. En la autenticación del servidor, el cliente autentifica el servidor primero solicitando el certificado de la llave pública del servidor. El cliente genera

un reto (llave), lo encripta con la llave del servidor y después se lo envía. El servidor retorna el reto desencriptando el mensaje usando la llave privada y después encripta el mensaje con el reto que el cliente le había enviado. La desencripción exitosa autentifica el servidor al cliente. El servidor puede retornar una autenticación al cliente solicitándole el certificado de llave pública. [Rajput, 2000]

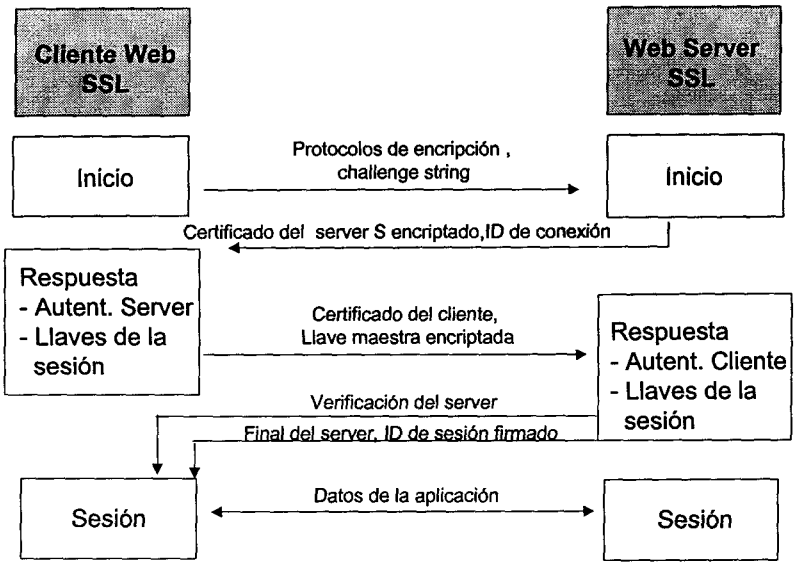


FIGURA 3.5. EJEMPLO DE SSL.

3.4.2 SECURE ELECTRONIC TRANSACTION (SET)

Desarrollados por VISA y MasterCard. Este protocolo es un método para asegurar el costo efectivo de las transacciones con tarjetas bancarias a través de redes. Incluye protocolos para compra de bienes y servicios electrónicamente, requiere la autorización del pago y solicita las "credenciales" (certificados).

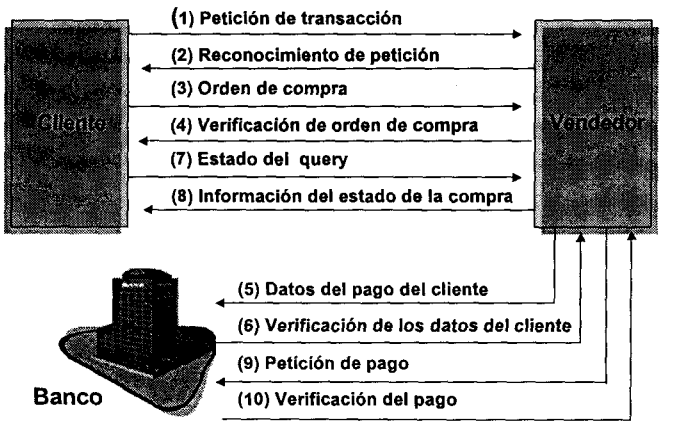


FIGURA 3.6. EJEMPLO DE SET

3.5 SEGURIDAD EN SISTEMAS OPERATIVOS

Los servicios que ofrece un sistema operativo es lo más complejo y flexible. Muchos servicios pueden incrementar la posibilidad de errores en la programación del sistema operativo y adicionar puertas traseras potenciales que permiten a intrusos obtener el control de la máquina. [Cameron, 1999]

3.5.1 UNIX

En la década de los ochenta para mucha gente el concepto de *seguridad* era algo inimaginable en el entorno Unix: la facilidad con que un experto podía acceder a un sistema, burlar todos sus mecanismos de protección y conseguir el máximo nivel de privilegio era algo de sobra conocido por todos, por lo que nadie podía pensar en un sistema Unix *seguro*. [Villalón, 2000]

Aunque en un principio y según uno de sus creadores, Unix no se diseñó para ser seguro, a finales de los 80 se convirtió en el primer sistema operativo en alcanzar niveles de seguridad *quasi* militares. En la actualidad se puede considerar el sistema operativo de propósito general más fiable del mercado; desde los clones habituales (Solaris, HP-UX, IRIX...) hasta los *'Trusted Unix'*, pasando por los sistemas gratuitos (Linux, FreeBSD...), cualquier entorno Unix puede ofrecer los mecanismos de seguridad suficientes para satisfacer las necesidades de la mayoría de instituciones. Los Unices habituales, como Solaris o Linux, son bastante inseguros tal y como se instalan por defecto (*out-of-the-box*), esto significa que requieren de una mínima puesta a punto, en cuanto a seguridad se refiere, antes de ponerlos a trabajar con unas mínimas garantías de fiabilidad. Una vez realizada esta puesta a punto suelen tener una seguridad aceptable en redes de propósito general. El problema es que en muchas ocasiones se pone a trabajar a Unix tal y como se instala por defecto, lo que convierte a cualquier sistema operativo, Unix o no, en un auténtico agujero en cuanto a seguridad se refiere: cuentas sin *password* o con *passwords* por defecto, servicios abiertos, sistemas de ficheros susceptibles de ser compartidos... [Villalón, 2000]

Dentro de la familia Unix existen una serie de sistemas denominados 'Unix seguros' o 'Unix fiables' (Trusted Unix); se trata de sistemas con excelentes sistemas de control, evaluados por la *National Security Agency* (NSA) estadounidense y clasificados en niveles seguros (B o A). Entre estos Unix seguros podemos encontrar AT&T System V/MLS y OSF/1 (B1), Trusted Xenix (B2) y XTS-300 STOP 4.1 (B3), considerados los sistemas operativos más seguros del mundo (siempre según la NSA). La gran mayoría de Unices (Solaris, AIX...) están clasificados como C2, y algunos otros, como Linux, se consideran sistemas C2 *de facto*: al no tener una empresa que pague el proceso de

evaluación de la NSA no están catalogados, aunque puedan implementar todos los mecanismos de los sistemas C2. [Villalón, 2000]

3.5.2 WINDOWS NT

Windows NT tiene una cuenta similar a la de root de sistemas Unix. La cuenta del *administrador* tiene privilegios de acceso similar a la usada en la cuenta root de Unix y puede modificar el registro, que incluye todos los passwords del sistema. Se recomienda que se renombre o deshabilite la cuenta de administrador.

Windows NT tiene características de seguridad, pero el administrador debe habilitarlas. Entre las características que ofrece, es una herramienta para monitorear Windows NT y hacer la seguridad más eficientemente. [Cameron, 1999]

3.6 SEGURIDAD EN CGI/API

Servidores de Web son programas excelentes, pero aplicaciones innovadoras existentes en la WWW requieren que los servidores sean extendidos con programas construidos específicamente. Desgraciadamente, estos programas pueden tener desperfectos que permitan ataques que comprometan el sistema.

Common Gateway Interface (CGI) fue el primer y es el más popular que extiende los servidores Web. Programas CGI corren como sub-tareas en el servidor de Web; argumentos son puestos en variables de entorno y en la entrada estándar del programa; los resultados son regresados por la salida estándar del programa. Los programas CGI han sido escritos ejecutar cadenas de base de datos y desplegar resultados; que permite ejecutar cálculos financieros complejos; y permite a los usuarios chatear con otros en el Internet.

Una nueva manera de extender los servidores de Web es con el uso de Application Programmer Interfaces (APIs). API es una manera rápida de conectar programas específicos al servidor de Web porque no requiere que nuevos procesos sean iniciados para cada iteración Web. El propio servidor Web ejecuta el código de la aplicación dentro de su espacio de direccionamiento que es invocado a través de una conexión registrada.

Como resultado de su poder, las interfaces CGI y API puede comprometer la seguridad del servidor Web y del host donde se esta ejecutando. Esto es porque cualquier programa puede correr a través de esta interfase. Esto puede incluir programas que tiene problemas de seguridad, programas que dan acceso a

externos a la computadora, e igual programas que pueden cambiar o borrar los archivos críticos del sistema.

Dos técnicas pueden ser usadas para limitar el daño que puede hacerse por medio de un CGI y un API:

- Los programas por si mismos deben ser diseñados e inspeccionados para asegurar que pueden ejecutar sólo las funciones deseadas.
- Los programas deben correr en un ambiente restringido. Si estos programas pueden ser destruidos por atacantes para hacer algo inesperado, el daño que ellos pueden hacer será limitado.

En los sistemas operativos que permiten correr múltiples usuarios en múltiples niveles autorizados, servidores Web corren bajo una cuenta restringida. Programas que son extendidos en el servidor Web, a través de interfases CGI o API, son ejecutados también en la misma cuenta restringida.

Desgraciadamente, otros sistemas operativos no tienen el mismo concepto de usuarios restringidos. En sistemas operativos Windows 3.1/95/98/Me y Macintosh, no hay una manera sencilla de tener un sistema operativo restringido para poner un programa CGI. [Garfinkel, 1997]

3.7 SEGURIDAD EN LEGUAJES DE PROGRAMACIÓN

3.7.1 JAVA / JAVASCRIPT

Java y JavaScript son lenguajes para agregar interactividad en páginas Web. Ambos lenguajes pueden correr un visualizador Web o en un servidor Web. Ambos lenguajes tiene una sintaxis parecida al lenguaje C++.

A pesar de esta similar apariencia, Java y JavaScript son actualmente dos lenguajes completamente diferentes con diferentes semánticas, diferentes comunidades de usuarios, y diferentes implicaciones de seguridad. [Garfinkel, 1997]

3.7.1.1 JAVA

Java no fue diseñado para ser un lenguaje de programación seguro. Bajo la visión original de Java, programas solo serían bajados por un equipo de

manufactura o por un proveer aprobado. Java fue diseñado para una comunidad de programadores cerrada y para cierto ambiente.

Cuando Java fue reposicionado para la Web, la seguridad inmediatamente se volvió una preocupación. Por diseño, la WWW permite que cualquiera baje cualquier página de cualquier lugar de Internet, si esta es de un proveedor aprobado o no. Si lo usuarios de la Web pueden bajar y correr un programa simplemente presionado en una página Web, entonces la necesidad de algunos mecanismos para proteger a los usuarios de programas maliciosos. [Garfinkel, 1997]

3.7.1.2 JAVASCRIPT

Programas en JavaScript debe ser esencialmente más seguros que los programas escritos en Java o en otros lenguajes de programación por diferentes razones:

- No hay métodos de JavaScript que puedan accesar directamente por el cliente de un sistema de archivos de una computadora.
- No hay métodos de JavaScript que directamente puedan abrir conexiones a otras computadoras en la red.

Pero JavaScript, como otras partes en la red, esta cambiando. Netscape reporta un sistema que determina que privilegios permite un programa en JavaScript.

Problemas de seguridad han sido reportados con JavaScript. Esto es porque la seguridad es más que protección contra la divulgación de la información o modificación de archivos locales.

3.7.2 PERL

Perl es un lenguaje optimizado para examinar archivos de texto arbitrario, extraer información de esos archivos, e imprimir reportes basados en esa información. Es también un buen lenguaje para muchas tareas de administración de sistema. El lenguaje intenta ser práctico(fácil de usar, eficiente, completo) en lugar de bonito(pequeño, elegante, mínimo).

Perl combina algunas de las mejores características de C, por lo que a la gente familiarizada con este lenguaje debe facilitársele aprender Perl. Sintaxis de

expresión correspondiente un poco a la sintaxis de expresiones en C. Al contrario de la mayoría de utilerías en Unix, Perl no limita arbitrariamente el tamaño de los datos si se tiene la memoria, Perl puede meter todo tu archivo en una simple cadena. La recursividad es ilimitada y las tablas usadas por hashes crecen como sea necesario para prevenir desempeño degradado. Perl usa técnicas de patrones sofisticados de verificación de grandes cantidades de datos rápidamente. Además de estar optimizado para examinar texto, Perl puede también trabajar con datos binarios, y puede hacer que archivos dbm parezcan hashes. Los scripts de Perl son más seguros que los programas de C a través de un mecanismo de seguimiento que previene muchos hoyos de seguridad. [Kassab]

3.8 SEGURIDAD EN LA CONEXIÓN

Una forma popular de asegurar las conexiones de red es usar conexiones encriptadas. Encripción en la conexión se refiere a la encripción en la capa de enlace de datos y proporciona encripción total a todos los datos que pasan entre dos terminales de red. Encriptores de la conexión pueden ser agregados enfrente de los dispositivos de red tal como ruteadores, truncales PBX, y multiplexores. Los encriptores de la conexión emplean una variedad de algoritmos populares (ej. RSA, DES). Estos encriptores son usualmente transparentes para una red especifica o protocolo de aplicación usado. En construcciones WAN, encriptores de la conexión usualmente soportan altas velocidades de datos para mejorar la transparencia de las operaciones de red.

Encripción en la conexión proporciona una de los métodos más seguros de conectividad y es casi imposible que se pueda escuchar en una conexión o se pueda suplantar a un usuario. Sin embargo, es muy caro poner esta forma de seguridad y mantenerla. Si los dos sitios pertenecen a dos diferentes organizaciones, ambos tiene que estar de acuerdo en instalar los encriptores en ambos lados. [Rajput, 2000]

3.9 HERRAMIENTAS DE MONITOREO

3.9.1 SNIFFERS

Un sniffer se podría resumir como un programa que lo que hace es capturar todos los datos que pasan a través de una tarjeta de red. Para ello se basa en un defecto del protocolo ethernet (el que se usa normalmente en las redes locales). Este protocolo lo que hace es mandar la información a todos los ordenadores de la red, aunque no vaya dirigida a ellos, luego son los propios ordenadores los que

basándose en la cabecera del paquete ethernet aceptan el paquete o no, según vaya dirigido a ellos o no. Normalmente todas las redes tienen este defecto, aunque se puede evitar, ethernet normalmente manda los paquetes de datos a todas las estaciones de la red, entonces lo que hace el sniffer es poner la tarjeta en modo promiscuo. El modo promiscuo significa que la tarjeta capturara todos los paquetes ethernet, aunque no vayan dirigidos a ella. [Raise]

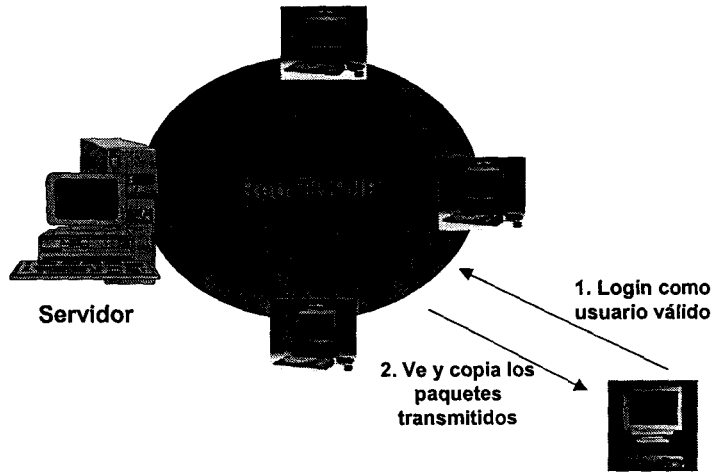


FIGURA 3.7. EJEMPLO DE SNIFFER.

3.9.2 SCANNERS

Como su nombre lo indica se trata de programas que permiten rastrear la red en busca de puertos abiertos por el cual acceder y manipular un sistema o introducir un virus o trayano.

3.9.3 DETECTORES DE INTRUSOS

Son herramientas usadas para la colección de acontecimientos relacionados con el sistema y la red acceso. También deben dar una señal de alarma en el caso que se detecte algún peligro, como actividades no autorizadas y maliciosas dejando al sistema, aplicaciones y datos seguros del mal uso y abuso. Si estos sistemas son amenazados, estas herramientas pueden notificar al administrador de red e incluso tomar acciones preventivas para evitar que la información sea robada o se pierda.

CAPITULO 4

METODOLOGÍA

El objetivo de este capítulo es dar una descripción general de los escenarios implementados en el laboratorio. La configuración detallada de cada uno de los escenarios se incluye en los anexos.

4.1 ESCENARIO 1: E_COMMERCE SOBRE IPv4

Se desarrolló un pequeño sitio para simular E_Commerce. La finalidad de este sitio es vender cursos a estudiantes de la universidad simulada o estudiantes de otras universidades que tengan convenio con esta universidad. En el anexo A se da una descripción más amplia del sitio y las políticas seguidas.

El sitio se monto sobre el siguiente equipo:

- *mainipv6.ipv6.com.mx*

Características:

Linux RedHat 6.1
3ffe:1200:300a:2::9
131.178.107.9
Servidor web Apache2 (IPv4/IPv6)
DNS, primario para ipv6.com.mx (IPv4/IPv6)

El servidor funciona para IPv4 y IPv6, pero para fines de este escenario solo se contemplo IPv4.

Solo se monto el sitio en el servidor y se dejaron las medias de seguridad que trae por default el sistema operativo, no se agrego alguna herramienta de seguridad.

4.2 ESCENARIO 2: E_COMMERCE SOBRE IPv4 UTILIZANDO IBM SET DEMO

Para la implementación de este escenario se hizo una búsqueda profunda en libros e Internet de una versión libre o demo del protocolo SET, encontrando una versión demo de IBM el cual se describe a continuación:

El IBM SET demo permite evaluar los certificados SET para la Cartera (Wallet), Comerciante (Merchant) y el Portal de Pagos (Payment Gateway) SET.

El demo IBM SET proporciona acceso al Comerciante de prueba y al Portal de Pagos (Merchant y Payment Gateway) para que sea evaluado por la Cartera (Merchant) de prueba. El Comerciante y el Portal de Pagos se encuentran en sitios de IBM y la Cartera fue bajada desde el sitio de MasterCard en la siguiente dirección: http://www.mastercard.com/th/wallet/index.html.

El Portal de comunicación se encuentra disponible las 24 horas del día y los 7 días de la semana con excepción de 9:00 a 10:00 de la mañana tiempo Este los días viernes ya que se encuentra en mantenimiento y respaldo.

IBM y MasterCard proporcionan el IBM Consumer Wallet 2.1 (Cartera de Consumo IBM 2.1) – una Cartera Electrónica para transacciones de e_commerce para clientes.

Características:

1. Compatible con ECML (Electronic Commerce Modeling Language) en el mercado. ECML es la estandarización de las formas de orden en línea del comerciante que permite a los monederos hacer un llenado automático de la información del cliente.
2. Soporte de SSL y SET (encripción de comercio electrónico y protocolos de seguridad).
3. Disponible en 24 idiomas.
4. IBM puede proveer comercio a través de todo el mundo, distribución y soporte para la Cartera de los miembros de MasterCard.

Por la forma en que se proporciona esta demo el Comerciante y el Portal de Pagos se encuentran en sitios de IBM y la Cartera fue bajada desde el sitio de MasterCard en la computadora personal del tesista, en donde se hizo la evaluación del mismo.

El detalle del funcionamiento del demo se expone en el anexo B.

4.3 ESCENARIO 3: E_COMMERCE SOBRE IPv4 UTILIZANDO VPN

En este escenario se utilizo la VPN implementada para la tesis "Utilización de VPNs (Virtual Private Networks) como mecanismo de transferencia de información seguro en Instituciones Educativas" de Miriam Victoria Chan Pavón, dicha tesis se desarrollo a la par de esta y se apoyo en la implementación de la VPN.

El equipo utilizado fue un servidor para la VPN y una laptop para hacer las conexiones del cliente, las características de los equipos son las siguientes:

- medusa.mty.itesm.mx

  Características:

  Sistema Operativo Windows 2000 Server.
  IP: 131.178.21.42
  Computadora Intel Pentium III de 1 GHz.
  Disco duro de 30 GB.
  Memoria RAM de 256 MB.

- Laptop sin dominio.

  Características:

  Sistema Operativo Windows 2000 Profesional.
  Dirección IP dinámica.
  Computadora Intel Celeron de 700 MHz.
  Disco duro de 10.0 GB.
  Memoria RAM de 64 MB.

Al servidor VPN se le instalo el servidor de Web Apache donde se monto el sitio desarrollado para simular e_commerce, el cual es descrito en el anexo A.

El servidor de VPN quedo habilitado tanto para conexiones de acceso remoto vía LAN o por Acceso telefónico, pero para fines de esta tesis sólo se hicieron pruebas y análisis vía LAN.

Dependiendo del tipo de Protocolo que se desee utilizar para la comunicación con el cliente de VPN se procede a su configuración. El Servidor de VPN habilita 128 puertos para conexiones PPTP y 128 para conexiones L2TP.

Point to Point Tunneling Protocol utiliza el protocolo Point to Point the Microsoft para la autentificación de usuarios y el protocolo de Encripción Point-toPoint, también de Microsoft para encapsular y encriptar el tráfico IP, IPX y NetBEUI. Se utiliza el Protocolo de Microsoft Challenge Handshake version 2 (MS-CHAP v2) para passwords fuertes asegurando de esta manera un conexión segura de VPN. Antes de establecer la conexión se solicita el nombre de usuario y su password para que sea autentificado, bajo este esquema no se requiere de una Autoridad Certificadora.

Layer Two Tunneling Protocol con IPSec utiliza el protocolo Point to Point para la autentificación de usuarios y el protocolo IPSec para encriptar y encapsular el trafico IP, IPX y NetBEUI. Esta combinación utiliza la autentificación de la identidad de la computadora basada en el uso de Certificados, para crear una asociación de seguridad entre los protocolos PPP e IPSec.

La configuración del cliente de VPN se realiza a través de Conexiones de Red y de Acceso telefónico en el panel de control del sistema operativo Windows 2000, se establece una nueva conexión y se le indica que la conexión es mediante VPN, después se configura el nombre o dirección IP del Servidor de VPN.

En el anexo C se hace una descripción detalla de la configuración efectuada para el servidor VPN y el cliente.

4.4 ESCENARIO 4: E_COMMERCE SOBRE IPv6

La seguridad en IPv6 se implementa por medio de IPsec. IPsec se hace obligatorio en IPv6 ya que es el medio que proporciona la funcionalidad de autenticación y encripción de IPv6.

IPsec proporciona dos modos de funcionalidad básico: Transporte y Túnel, uno proporciona protección a la carga de IP pero no al paquete, y el otro proporciona protección al paquete completo de IP.

Para implementar el modo túnel se requiere un router y para el modo de transporte sólo se requieren dos hosts, por limitantes de acceso al equipo sólo se implemento el modo de transporte.

El modo de transporte con IPv6 requirió dos equipos los cuales se describen a continuación:

- *ipsec.ipv6.itesm.mx*

  Características:

  FreeBSD 4.4
  3ffe:8241::210:4bff:fe27:2048
  131.178.107.204
  Servidor Web Apache2 (IPv4/IPv6)

- Laptop sin dominio

  Características:

  FreeBSD 4.4
  3ffe:8241::248:54ff:fec0:b87
  131.178.107.202
  Servidor Web Apache2 (IPv4/IPv6)

Como se podrá observar en las características del equipo, los dos tiene sistema operativo FreeBSD, adicionalmente se instalo el proyecto kame el cual es un esfuerzo para crear un software sólido especializado en IPv6/IPsec, en conjunto el sistema operativo y el proyecto kame nos proporciona la facilidad de implementar IPv6/IPsec.

La configuración del modo de transporte se efectuó entre dos hosts con las siguientes características de configuración:

AH Algoritmo	MD5
AH Modo del algoritmo	Keyed
AH Transformada	RFC 1828
AH Llave	128 bits
AH Modo	Todo el datagrama
ESP Algoritmo	3DES
ESP Modo del algoritmo	CBC
ESP Transformada	RFC 2451
ESP Llave	192 bits
ESP Modo	Transporte

TABLA 4.1 CARACTERÍSTICAS DE CONFIGURACIÓN DEL MODO DE TRANSPORTE.

ESP en modo de transporte entre Host-A y Host-B.

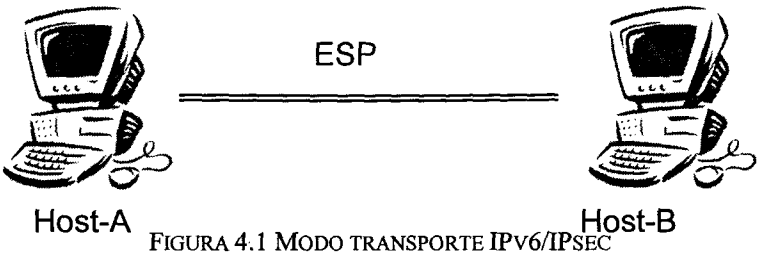


FIGURA 4.1 MODO TRANSPORTE IPV6/IPSEC

En el anexo D sección 1 se expone la configuración detallada del esquema anteriormente.

Adicionalmente al laboratorio descrito en la parte anterior se hizo una investigación profunda en Libros e Internet de proyectos de investigación sobre seguridad en IPv6, encontrando dos proyectos, Kame y Tahi, los cuales hacen investigación en seguridad sobre IPv6.

El proyecto kame es un esfuerzo conjunto de empresas japonesas en su mayoría para proporcionar un software sólido especializado en IPv6/IPsec. El proyecto proporciona referencia libre de IPv6 e IPsec desarrollado en FreeBSD, NetBSD, OpenBSD y BSDI.

El proyecto TAHI es un esfuerzo conjunto formado con el objetivo de desarrollar y proporcionar la verificación de la tecnología de IPv6.

Busca y desarrolla pruebas de adaptabilidad e interopabilidad para IPv6. El proyecto TAHI trabaja muy cerca del proyecto KAME, ayuda a las actividades de calidad ofreciendo la verificación de la tecnología IPv6 y mejorar el desarrollo eficientemente.

Los resultados y frutos están abiertos al público de manera libre. Cualquier desarrollador interesado en IPv6 puede utilizar los resultados y frutos del proyecto TAHI libremente. Proporcionar la verificación de la tecnología libremente contribuye al avance de IPv6.

Las organizaciones que forman el proyecto son, The University of Tokio, YDC Corp. y Yokogawa Electric Corp.

El proyecto consta de dos paquetes, la herramienta de prueba de adaptabilidad de IPv6 (v6eval) y el paquete de prueba de adaptabilidad de IPv6 (ct).

V6eval es una herramienta que puede generar y verificar cabeceras entre las que destacan para fines de la tesis, la cabecera de autenticación (AH) y la cabecera de encapsulado de carga de seguridad (ESP) de IPv6.

Ct es el programa de prueba de adaptabilidad de IPv6. Las pruebas se ejecutan en la herramienta de adaptabilidad de IPv6 (v6eval).

La configuración de este segundo laboratorio y los resultados obtenidos se exponen en el anexo D parte 2.

4.5 ANÁLISIS DE RIESGOS Y VULNERABILIDADES

Para los escenarios descritos en este capítulo se aplicaron los mismos análisis de riesgos y vulnerabilidades y sniffeo.

Se utilizo la herramienta de análisis de riesgos y vulnerabilidades NetRecon ya que es una de las más completas en el mercado, además que se tuvo una licencia que permitía la utilización de todas sus funcionalidades.

A los servidores de los cuatro escenarios descritos en este capítulo se les aplico un scaneo de alto nivel mientras se hacía la simulación de e_commerce.

Para el sniffeo se utilizo la herramienta de ataque externo Ethereal también una de las completas en el mercado y de las pocas que soportan IPv6, esta es una herramienta libre y se puede hacer el uso completo de todas sus funcionalidades, además de que se puede instalar en la mayoría de la versiones Unix y Windows.

El sniffeo se realizo mientras se hacía la simulación de e_commerce y tratar de visualizar el número de tarjeta de crédito, elemento más importante en las transacciones.

En el anexo E sección 1 y 2 se exponen a detalle las dos herramientas utilizadas.

CAPITULO 5

RESULTADO DE LOS ANÁLISIS DE RIESGOS Y PRUEBAS DE SEGURIDAD EFECTUADOS EN IPv4 E IPv6

A los escenarios descritos en el capítulo 4 se les efectuó un análisis de riesgos el cual se realizó con la utilización de dos herramientas, NetRecon y Ethereal, una efectúa un análisis de vulnerabilidades y la otra hace una análisis de los paquetes que viajan en la red.

NetRecon asigna una vulnerabilidad en una escala de 1-100, las vulnerabilidades se dividen en tres categorías basándose en el riesgo que estas representan: Bajo riesgo (1-33), Medio (34-66), y Alto (67-100).

Ethereal trata de detectar si la información viaja en texto en claro o con algún protocolo de encripción, si encuentra que viaja con algún protocolo de encripción trata de obtener la mayor información posible y descriptarla.

5.1 ESCENARIO 1: E_COMMERCE SOBRE IPv4

5.1.1 ANÁLISIS DE RIESGOS

Para este escenario no se encontraron vulnerabilidades de alto riesgo, el mayor número de vulnerabilidades encontradas fueron de nivel bajo y un número menor de nivel medio.

Se detectaron 5 vulnerabilidades de nivel medio que básicamente se relacionan a tres, la primera tiene un valor de 42 y las dos restantes un valor de 39:

- HTTP habilitado. La herramienta detecta que el servicio de http se encuentra habilitado y la solución que propone es deshabilitar el servicio sino es utilizando, pero para este caso no aplica la solución, ya que se requiere que el servicio se encuentre habilitado, otra solución es restringir el

acceso a este servicio y el sitio el cual se simula tiene una política de acceso de cuenta y password.

- SSH. La herramienta detecta que se encuentra un servicio de un producto de software, este servicio es el Secure Shell, es un servicio que se encuentra habilitado para hacer accesos remotos seguros al servidor, la recomendación que propone la herramienta es considerar los beneficios del producto identificado y hacer una balance contra el riesgo de seguridad, esta herramienta es conocida en el mercado como una herramienta segura por los algoritmos de encripción que maneja y el manejo de llaves públicas que utiliza.
- Apache. La herramienta detecta que se encuentra un servicio de un producto de software, este servicio es el servidor de Web instalado para proporcionar el servicio de http, la recomendación igual que la anterior es considerar los beneficios del producto identificado y hacer una balance contra el riesgo de seguridad, este servicio es elemental para el funcionamiento del sitio de e_commerce simulado.

Se detectaron 9 vulnerabilidades de nivel bajo entre las que destacan:

- DNS habilitado. Se detecta el servidor de nombres de dominio se encuentra habilitado con un valor de riegos 28, los servidores DNS son susceptibles a ataques spoofing que pueden cambiar o corromper el nombre de un dominio, la solución propuesta es verificar anormalidades en los nombres o resolución de direcciones IP, poner otros servidores DNS autorizados en la red y buscar anormalidades.
- Puertos TCP abiertos. Algún puerto que presta un servicio que pueden permitir actividad no autorizada y tiene un valor de riesgo 14. Para la solución de esta vulnerabilidad se recomienda verificar que servicio se está prestando y si no es necesario deshabilitarlo.

En la siguiente tabla se exponen las principales vulnerabilidades encontradas a este escenario:

Tipo de Riesgo	Nivel	Nombre de la Vulnerabilidad	Descripción
Medio	42	HTTP	Servicio http habilitado.
	39	Servicio identificado	Servicio de un producto de software identificado.
Bajo	28	DNS habilitado	Servidor DNS que contiene nombres y direcciones IP.
	19	SSH habilitado	El servicio SSH proporciona autenticación a accesos remotos a través de una sesión encriptada.
	16	Identificación de un recurso de red.	Se puede obtener información que ayuda a identificar un recurso de red en particular en este caso el nombre de dominio de la dirección IP.
	15	ICMP	Respuesta utilizando el protocolo ICMP.
	14	Puerto TCP abierto	Este servicio permite actividad no autorizada dependiendo del puerto que se encuentre abierto

TABLA 5.1 VULNERABILIDADES ENCONTRADAS EN EL ESCENARIO 1

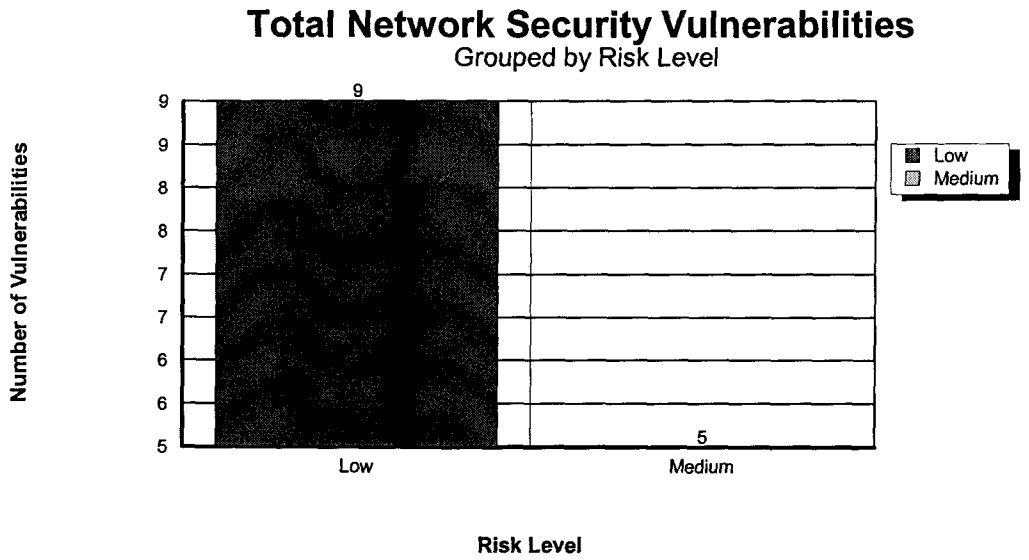


FIGURA 5.1 VULNERABILIDADES DEL ESCENARIO 1 AGRUPADAS POR NIVEL DE RIESGO

5.1.2 PRUEBAS DE SEGURIDAD

Las pruebas de seguridad se llevaron a cabo por medio de la herramienta de snnifing Ethereal, en la cual se detecto que para este escenario la información

es totalmente visible, viaja en texto en claro, la cuenta y password del control de acceso y el número de tarjeta de crédito son totalmente visibles.

En la siguiente figura se puede observar las dos direcciones IP, la origen y destino, además detecta que es protocolo HTTP simple y cual fue la tarea ejecutada en ese paquete en especial:

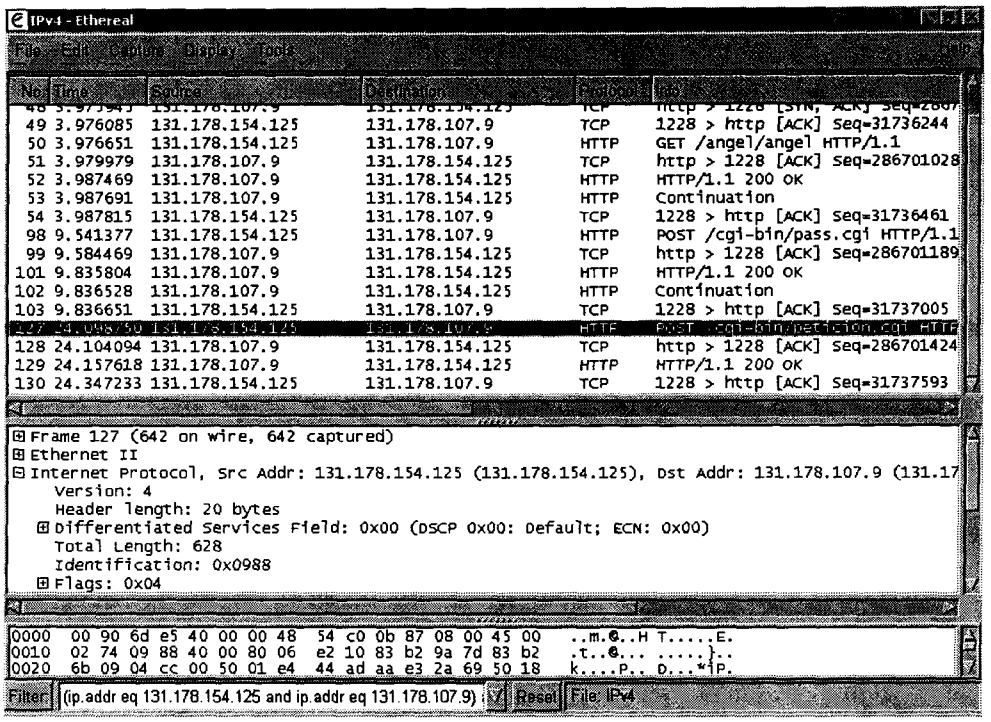


FIGURA 5.2 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 1

Una de las cuentas y password de uno de los alumnos simulados fue, usuario *alex* y password *lluvia*, como se puede observar en la siguiente figura esta información es totalmente visible:

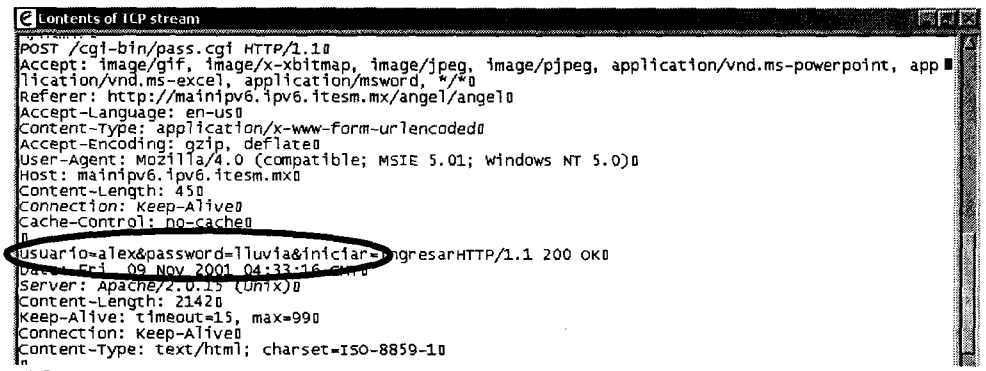


FIGURA 5.3 PANTALLA DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 1 VISUALIZANDO CUENTA Y PASSWORD

Otro elemento importante fue el número de tarjeta de crédito que se utilizo para la compra de un curso, el número simulado fue el 0001 0002 0003 0004, como se puede observar en la siguiente figura el número es totalmente visible:

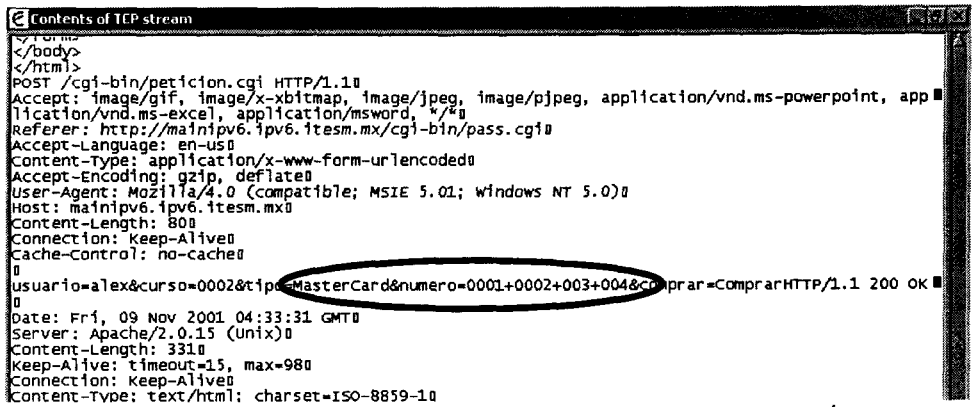


FIGURA 5.4 PANTALLA DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 1 VISUALIZANDO NÚMERO DE TARJETA DE CRÉDITO

5.2 ESCENARIO 2: E_COMMERCE SOBRE IPv4 UTILIZANDO IBM SET DEMO

5.2.1 ANÁLISIS DE RIESGOS

Para este escenario no se encontraron vulnerabilidades de alto riesgo, el mayor número de vulnerabilidades encontradas fueron de nivel bajo y un número menor de nivel medio.

Se detectaron 3 vulnerabilidades de nivel medio que básicamente se relacionan a dos, la primera tiene un nivel de riesgo 42 y la segunda tiene un 39:

- HTTP habilitado. La herramienta detecta que el servicio de http se encuentra habilitado y la solución que propone es deshabilitar el servicio sino es utilizando, pero para este caso no aplica la solución, ya que se requiere que el servicio se encuentre habilitado, otra solución es restringir el acceso a este servicio.
- Apache. La herramienta detecta que se encuentra un servicio de un producto de software, este servicio es el servidor de Web instalado para proporcionar el servicio de http, la recomendación es considerar los beneficios del producto identificado y hacer una balance contra el riesgo de seguridad, este servicio es elemental para el funcionamiento del sitio de e_commerce simulado por IBM.

Se detectaron 4 vulnerabilidades de nivel bajo entre la que destaca:

- Puerto TCP abierto. Algún puerto que presta un servicio que pueden permitir actividad no autorizada y tiene un valor de riesgo 14. Para la solución de esta vulnerabilidad se recomienda verificar que servicio se está prestando y si no es necesario deshabilitarlo.

En la siguiente tabla se exponen las principales vulnerabilidades encontradas a este escenario:

Tipo de Riesgo	Nivel	Nombre de la Vulnerabilidad	Descripción
Medio	42	HTTP	Servicio http habilitado.
	39	Servicio identificado	Servicio de un producto de software identificado.
Bajo	16	Identificación de un recurso de red.	Se puede obtener información que ayuda a identificar un recurso de red en particular en este caso el nombre de dominio de la dirección IP.
	14	Puerto TCP abierto	Este servicio permite actividad no autorizada dependiendo del puerto que se encuentre abierto
	5	Dirección IP encontrada	Se descubrió la dirección IP de un recurso de red usando su nombre.

TABLA 5.2 VULNERABILIDADES ENCONTRADAS EN EL ESCENARIO 2

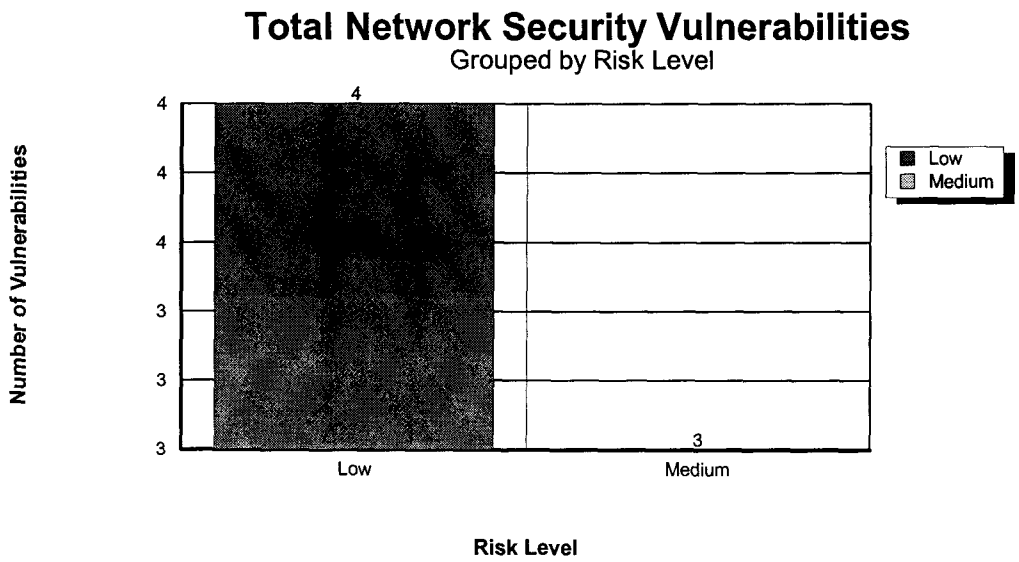


FIGURA 5.5 VULNERABILIDADES DEL ESCENARIO 2 AGRUPADAS POR NIVEL DE RIESGO

5.2.2 PRUEBAS DE SEGURIDAD

Para hacer las pruebas de seguridad en este escenario se simulo la compra de un artículo y el pago se hizo con tarjeta de crédito visa con número 110019767, dicha tarjeta de crédito es ficticia y fue proporcionada por el sitio de IBM para tener acceso a los servidores demo.

Los resultados de las pruebas de seguridad fueron que no se pudo visualizar el número de tarjeta de crédito, elemento principal a proteger.

A continuación se muestra las figuras que visualizan como se ven los paquetes, en la primera se puede ver que la herramienta detecta las dos direcciones entre las que se hizo la transacción, además detecta el protocolo SSL versión 3:

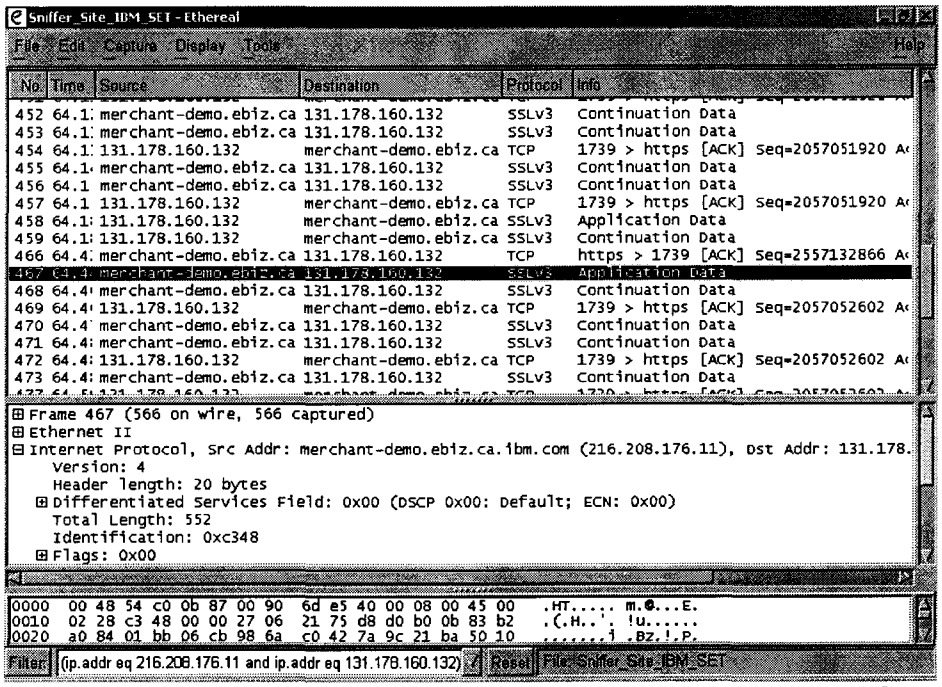


FIGURA 5.6 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 2

En la siguiente figura se presenta la información que fue captada por la herramienta, como se puede observar la información no es entendible:

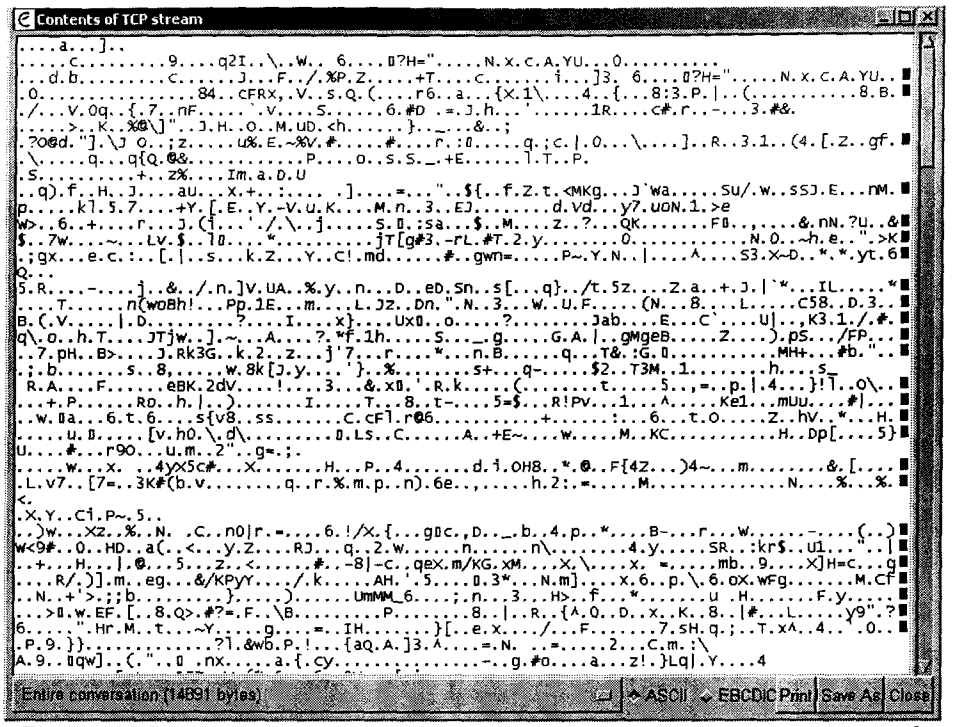


FIGURA 5.7 PANTALLA DE UN PAQUETE DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 2

5.3 ESCENARIO 3: E_COMMERCE SOBRE IPv4 UTILIZANDO VPN

5.3.1 ANÁLISIS DE RIESGOS

Se encontraron dos vulnerabilidades de alto Riesgo en este servidor con una valor de 86 de la escala de Alto riesgo, ambas se encuentran en el SMTP el cual permite ejecuciones remotas de comandos vía filtros, este principalmente afecta a sistemas Unix que no es el caso de este servidor. La recomendación de la Herramienta es la de verificar si este servidor soporta filtros, ya que si este servidor no los soporta entonces no representa una vulnerabilidad para el sistema y por lo tanto no hay riesgo, otra recomendación sería la de actualizar o reemplazar el servidor de SMTP.

Se detectaron 32 vulnerabilidades de nivel medio entre las que destacan:

- Servicio echo habilitado. Este servicio devuelve cualquier paquete que el cliente envía, es susceptible a ataques que crean direcciones de retorno falsa, la solución propuesta es deshabilitar este servicio. Tiene un valor de nivel de riesgo 60.

- Ftp habilitado. File Transfer Protocol (Protocolo de transferencia de archivos) es un protocolo que permite la transferencia de archivos ente sistemas. La solución propuesta es obtener la ultima versión y no permitir accesos remotos, o bien deshabilitar el servicio si no es necesario. Tiene un valor de nivel de riesgo 42.
- HTTP habilitado. La herramienta detecta que el servicio de http se encuentra habilitado y la solución que propone es deshabilitar el servicio sino es utilizando, pero para este caso no aplica la solución, ya que se requiere que el servicio se encuentre habilitado, otra solución es restringir el acceso a este servicio. Tiene un valor de nivel de riesgo 39.
- Apache. La herramienta detecta que se encuentra un servicio de un producto de software, este servicio es el servidor de Web instalado para proporcionar el servicio de http, la recomendación es considerar los beneficios del producto identificado y hacer una balance contra el riesgo de seguridad, este servicio es elemental para el funcionamiento del sitio de e_commerce simulado. Tiene un valor de nivel de riesgo 39.

Se detectaron 52 vulnerabilidades de nivel bajo entre las que destacan:

- Puertos TCP abiertos. Algún puerto que presta un servicio que pueden permitir actividad no autorizada y tiene un valor de riesgo 14. Para la solución de esta vulnerabilidad se recomienda verificar que servicio se está prestando y si no es necesario deshabilitarlo.

Algunos servicios los configura por defecto el servidor y la solución es deshabilitar ese servicio en particular, se recomienda que si algún servicio no es necesario deshabilitarlo para que de esta forma no se exponga al servidor a ataques.

En la siguiente tabla se exponen las principales vulnerabilidades encontradas a este escenario:

Tipo de Riesgo	Nivel	Nombre de la Vulnerabilidad	Descripción
Alto	86	SMTP	Permite ejecuciones remotas de comandos via filtros.
Medio	60	Echo Chargen	Este servicio devuelve cualquier paquete que el cliente envia. Este servicio causa que el servidor de TCP este enviando continuamente flujo de caracteres hasta que el cliente cierre la conexión
	45	SMTP	Servicio para el envió de mensajes electrónicos utilizando nombres de usuarios validos.
	44	Null sesions	Servicio de Permiso de sesiones anónimas
	42	File sharing ftp telnet nntp nbsession http	Servicio de Compartición de Archivos Servicio de Transferencia de Archivos Servicio de facilidad de ejecuciones remotas Servicio de recursos de la red Servicio de Servidor de Bloques de mensajes y recursos de la red Servidor de Web
	39	http ftp	Identificación de Servicios de Aplicación por Software.
	35	http Apache	Servicio de Web susceptible a acceso remoto contenido de directorios
Bajo	28	DNS	Servicio de Servidor de Nombres de Dominio
	20	SMTP ICMP	Conexiones rápidas por medio de SMTP Respuesta a peticiones UDP via ICMP
	16	ICMP	Respuesta a peticiones timestamp de ICMP Servicio que identifica los recursos de la red
	15	ICMP	Respuesta a comando ping y peticiones que identifican los recursos de la red Servicio de descartar
	14	TCP	Este servicio permite actividad no autorizada dependiendo del puerto que se encuentre abierto la mayoría de estos puertos y servicios son los de la vulnerabilidad 42

	11	Qotd Daytime	Permite enviar una cita al cliente cuando se añade al servidor Proporciona información del OS existente
	10	IP	Descubrimiento de la IP del recurso de red
	9	SMTP	Soporta protocolo EHLO o ESMTP
	5	IP	Descubrimiento de la IP por medio del nombre

TABLA 5.3 VULNERABILIDADES DEL ESCENARIO 3 AGRUPADAS POR NIVEL DE RIESGO

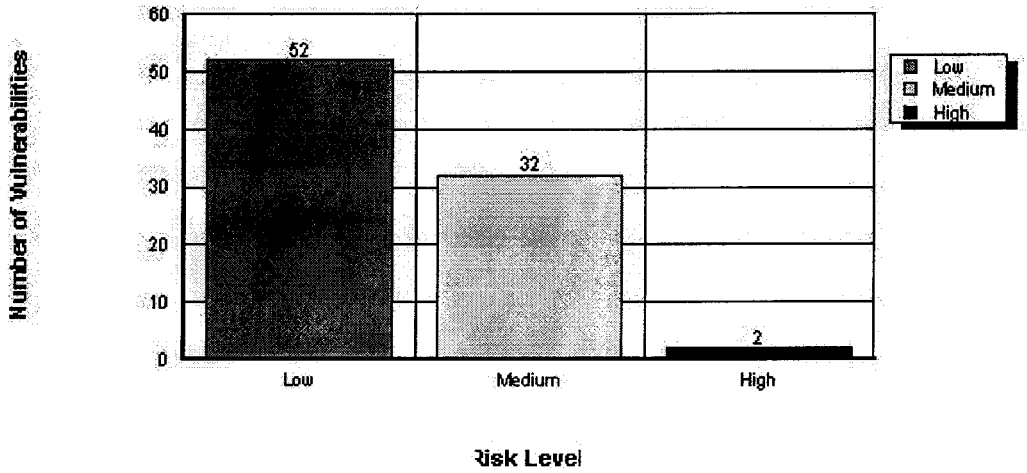


FIGURA 5.8 VULNERABILIDADES DEL ESCENARIO 3 AGRUPADAS POR NIVEL DE RIESGO

5.3.2 PRUEBAS DE SEGURIDAD

En este escenario se utilizaron dos protocolos el PPTP y el L2TP descritos en el capítulo anterior, a los dos esquemas se les aplico las mismas pruebas de seguridad obteniendo los mismos resultados.

Una de las cuentas y password de uno de los alumnos fue, usuario *alex* con password *lluvia*, dicha información no pudo ser visualizada o encontrada de manera visible.

El número de tarjeta de crédito que se utilizo para la compra de un curso fue el *0001 0002 0003 0004* que tampoco pudo ser visible en los paquetes capturados.

En la siguiente figura se puede observar que la herramienta detecta los paquetes del protocolo PPTP:

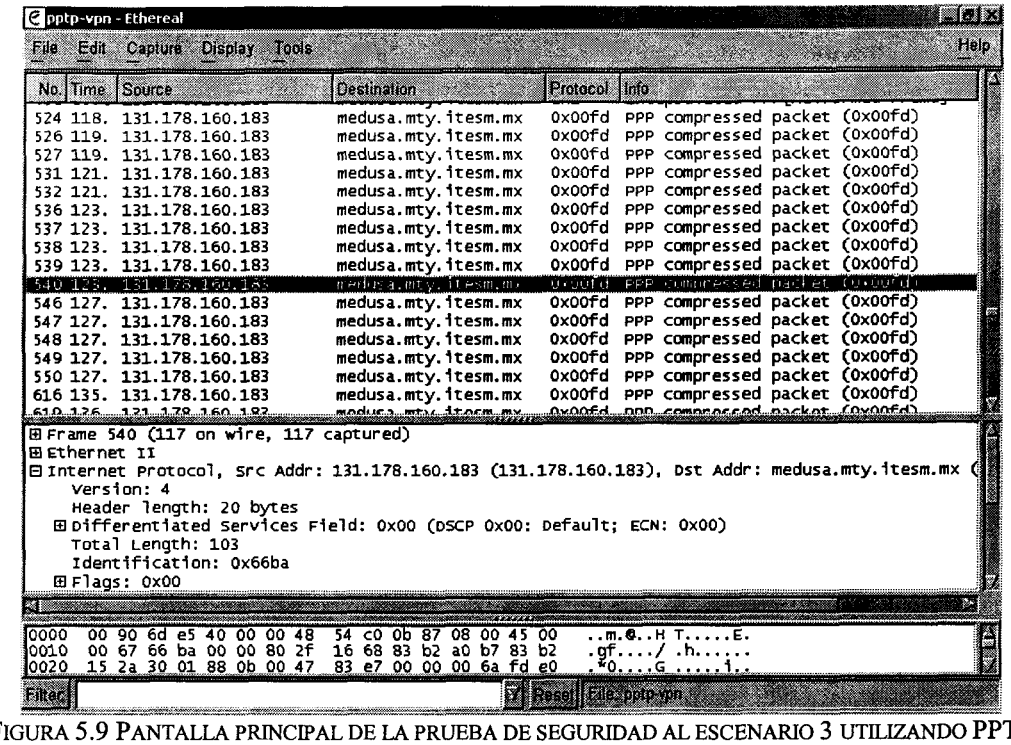


FIGURA 5.9 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 3 UTILIZANDO PPTP

En la siguiente figura se puede observar que la herramienta detecta que se esta utilizando el protocolo ESP, el cual es utilizado en L2TP:

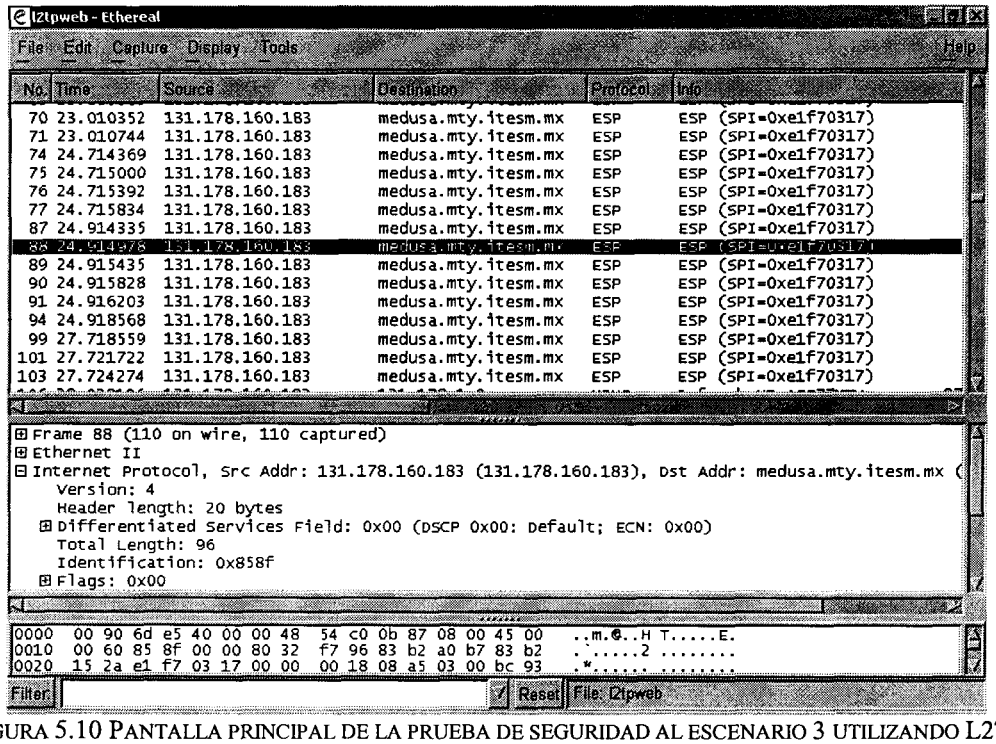


FIGURA 5.10 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 3 UTILIZANDO L2TP

5.4 ESCENARIO 4: E_COMMERCE SOBRE IPv6

5.4.1 ANÁLISIS DE RIESGOS

Para este escenario no se encontraron vulnerabilidades de alto riesgo, el mayor número de vulnerabilidades encontradas fueron de nivel bajo y un número menor de nivel medio.

Se detectaron 6 vulnerabilidades de nivel medio que básicamente se relacionan a tres, la primera tiene un valor de 42 y las dos restantes un valor de 39:

- Telnet habilitado. La herramienta detecta que el servicio de telnet se encuentra corriendo, la solución propuesta es deshabilitar este servicio si no es utilizado.
- HTTP habilitado. La herramienta detecta que el servicio de http se encuentra habilitado y la solución que propone es deshabilitar el servicio sino es utilizando, pero para este caso no aplica la solución, ya que se requiere que el servicio se encuentre habilitado, otra solución es restringir el acceso a este servicio y el sitio el cual se simula tiene una política de acceso de cuenta y password.
- Apache. La herramienta detecta que se encuentra un servicio de un producto de software, este servicio es el servidor de Web instalado para proporcionar el servicio de http, la recomendación igual que la anterior es considerar los beneficios del producto identificado y hacer una balance contra el riesgo de seguridad, este servicio es elemental para el funcionamiento del sitio de e_commerce simulado.

Se detectaron 8 vulnerabilidades de nivel bajo entre las que destacan:

- Puertos TCP abiertos. Algún puerto que presta un servicio que pueden permitir actividad no autorizada y tiene un valor de riesgo 14. Para la solución de esta vulnerabilidad se recomienda verificar que servicio se está prestando y si no es necesario deshabilitarlo.

En la siguiente tabla se exponen las principales vulnerabilidades encontradas a este escenario:

Tipo de Riesgo	Nivel	Nombre de la Vulnerabilidad	Descripción
Medio	42	Telnet habilitado	Telnet permite facilidades de ejecución remota con auntenticación basada en cuenta y password.
	42	HTTP	Servicio http habilitado.
	39	Servicio identificado	Servicio de un producto de software identificado.
Bajo	16	Identificación de un recurso de red.	Se puede obtener información que ayuda a identificar un recurso de red en particular en este caso el nombre de dominio de la dirección IP.
	15	ICMP	Respuesta utilizando el protocolo ICMP.
	14	Puerto TCP abierto	Este servicio permite actividad no autorizada dependiendo del puerto que se encuentre abierto

TABLA 5.4 VULNERABILIDADES ENCONTRADAS EN EL ESCENARIO 4

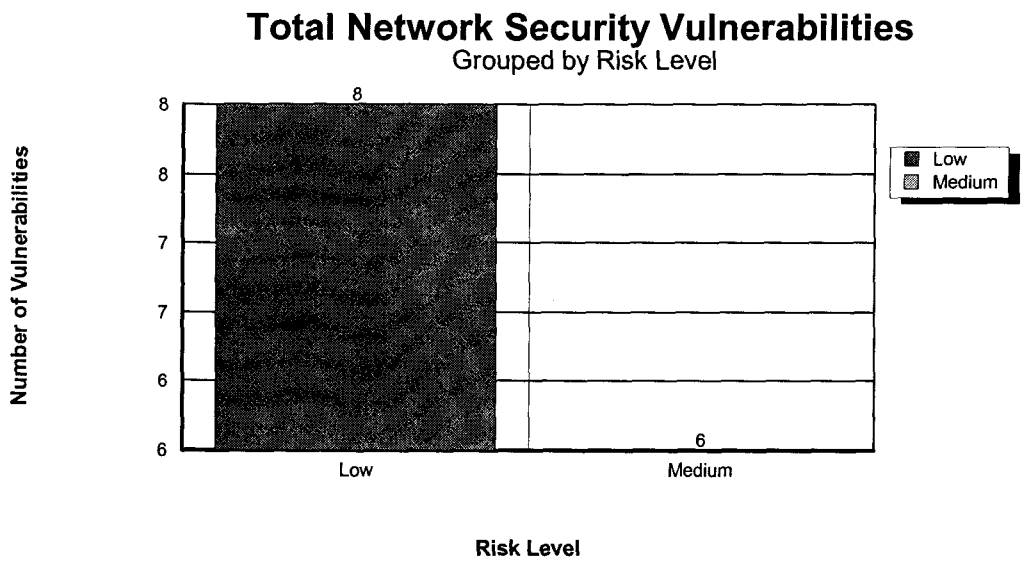


FIGURA 5.11 VULNERABILIDADES DEL ESCENARIO 4 AGRUPADAS POR NIVEL DE RIESGO

5.4.2 PRUEBAS DE SEGURIDAD

En este último escenario al igual que en los anteriores se utilizó la herramienta Ethereal, obteniendo como resultado que la información no puede ser desencriptada.

En la siguiente figura se puede ver que la herramienta detecta las dos direcciones IPv6 de los hosts que fuerón configurados para que la información que viaja entre ellos utilizara los protocolos AH y ESP, en el anexo D se puede corroborar las direcciones IP, la herramienta detecta que se esta utilizando el protocolo ESP para tratar de descencriptar la información, lo cual no pudo ser visible. Algunos datos como el número de asociación son detectados por la herramienta, para este escenario se configuro el SPI =0X00010001 tal como se muestra en la figura y puede ser corroborado en el anexo D.

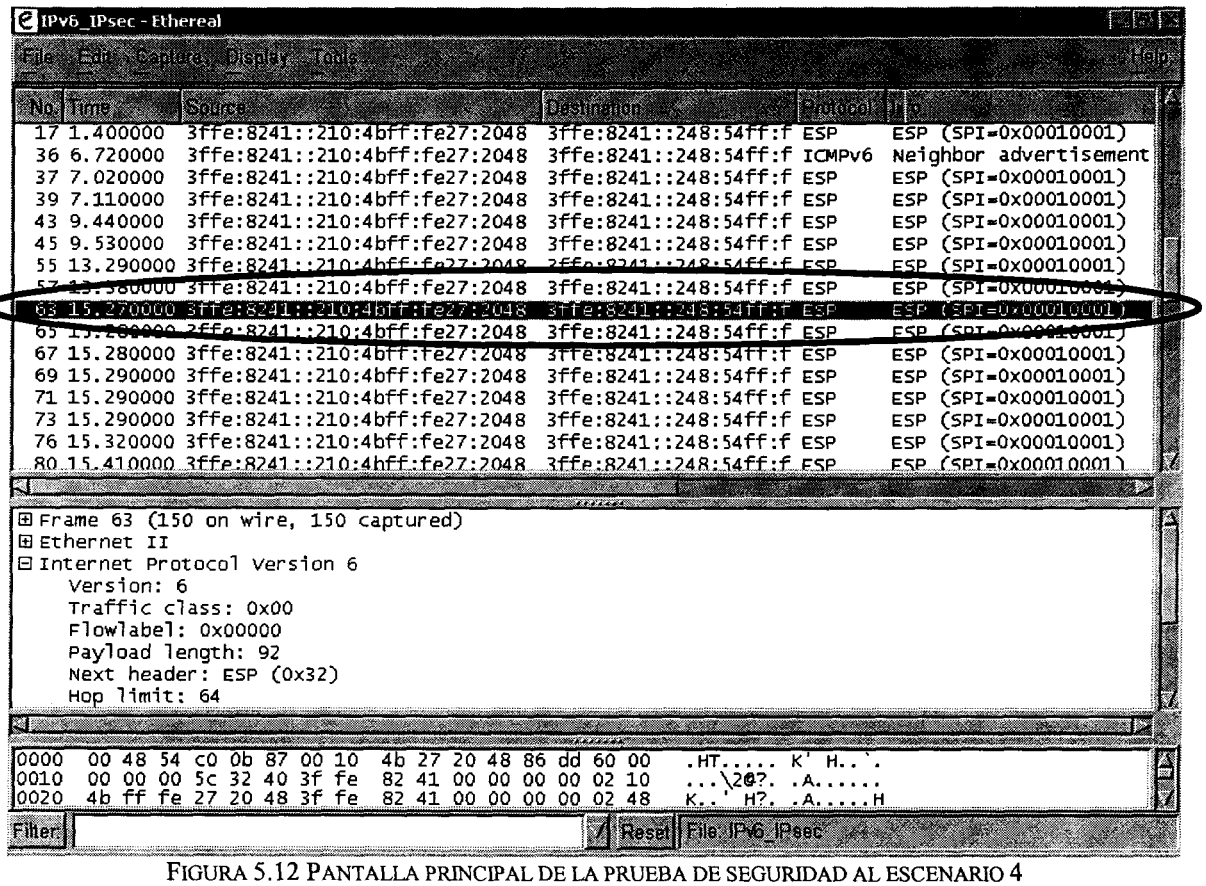


FIGURA 5.12 PANTALLA PRINCIPAL DE LA PRUEBA DE SEGURIDAD AL ESCENARIO 4

CAPITULO 6

CONCLUSIONES

6.1 CONCLUSIONES

Existen muy pocas aplicaciones que soportan IPv6, los principales navegadores de Internet como el Internet Explorer y Netscape no soportan IPv6, por lo cual si se quiere acceder a una página bajo IPv6 se requiere un visualizador especial, como el Mozilla de Netscape.

La calidad de la seguridad proporcionada por los protocolos de IPSec depende de varios factores. Los algoritmos de criptografía y validez de las llaves juegan un rol importante en IPSec tal como la implementación de los protocolos y administración de llaves en todos los participantes de los sistemas. La correcta implementación de los algoritmos es igual de importante. La seguridad de una implementación IPv6 depende parte en la seguridad del sistema operativo en donde IPv6 esta corriendo.

Como se pudo observar en los resultados de los análisis de riesgos del capítulo 5, las vulnerabilidades variaron en los diferentes sistemas operativos teniendo un número mayor en el sistema operativo Windows 2000 Server, la mayoría de las vulnerabilidades encontradas se pueden eliminar o reducir implementado políticas de seguridad en el sistema operativo.

Para eliminar vulnerabilidades dentro del sistema operativo se tiene que tener una buena administración de seguridad, se deben implementar políticas de seguridad que implican el cierre de puertos abiertos que no tienen ninguna funcionalidad importante o que no se requieren, deshabilitando servicios que el sistema operativo tiene habilitados por defecto y que no son usados, y/o separando servicios en distintos servidores. Dentro de la administración de seguridad también se requiere hacer una revisión periódica de la validez de las políticas implementadas en el pasado y si son necesarias nuevas.

Si la seguridad es proporcionada en la capa de red, se vuelve un servicio estándar que todas las aplicaciones pueden usar. El desarrollo de aplicaciones seguras se vuelve más simple. Es posible agregar seguridad transparentemente a las aplicaciones existentes si el software del protocolo de Internet es actualizado. Sería suficiente dar una instrucción al sistema operativo para que siempre ejecute

una asociación de seguridad antes de iniciar una conexión TCP o intercambio UDP. La seguridad es una parte integral en IPv6 y estará disponible en todas las plataformas.

Podemos concluir que la seguridad proporcionada por el protocolo de comunicaciones (IP) es mayor en cobertura con IPv6 que con IPv4, ya que para el escenario implementado con SET sobre IPv4 basa parte de su seguridad en SSL y las especificaciones de seguridad son suficientes para concluir que el protocolo IPv6 tiene características de seguridad para proporcionar una mejor autenticación y confidencialidad que SSL. Desde el punto de vista de red, los mecanismos de seguridad de IPV6 son usados para comunicaciones host-a-host, host-a-subred, subred-a-subred y los mecanismos de seguridad de SSL solo pueden ser usados en comunicaciones de host-a-host.

En el escenario 3 (IPv4 + VPN) se pudo observar que los protocolos utilizados para proporcionar seguridad en la transferencia de información son los protocolos PPTP el cual solo proporciona confidencialidad de los datos y L2TP que se basa en IPsec proporcionando confidencialidad e integridad de los datos, por lo tanto se puede concluir que IPv6 proporciona mayor seguridad que el protocolo IPv4 más VPN con conexión PPTP y la misma seguridad que IPv4 más VPN con conexión L2TP con la única diferencia de que este último no esta totalmente estandarizado para IPv4.

IPv6 ofrece como ventaja que solo se le tenga que agregar la funcionalidad de la VPN y SET, las herramientas pueden tomar el soporte de seguridad que proporciona IPv6.

En la siguiente tabla se puede ver en que capa del modelo TCP/IP u OSI se encuentran los mecanismos de seguridad implementados en los escenarios descritos en el capítulo 4, se agrega VPN en IPv6 ya que es un trabajo propuesto y no se incluye SET ya que aún no hay implementaciones sobre el nuevo protocolo.

TCP/IP	**Capa de Red**		**Internet**	**Transporte**		**Aplicación**	
OSI	**Física**	**Enlace de datos**	**Red**	**Transporte**	**Sesión**	**Presentación**	**Aplicación**
IPv4			IPSEC	SSL		SET	
			VPN (PPTP, L2TP)				
IPv6			IPSEC				
			VPN				

TABLA 6.1 MECANISMOS DE SEGURIDAD IMPLEMENTADOS Y SU CAPA DEL MODELO TCP/IP U OSI

En lo referente a la hipótesis podemos ver que para la primera parte del escenario 3, la VPN implementa la seguridad con el protocolo PPTP proporcionando solo confidencialidad de los datos y dado que IPv6/IPsec proporciona integridad y confidencialidad de los datos se concluye que para esta parte del escenario la hipótesis se cumple.

Para la segunda parte del escenario 3, la VPN implementa la seguridad con el protocolo L2TP el cual se basa en el protocolo IPsec sobre IPv4 y dado que IPv6 también proporciona su seguridad con el protocolo IPsec, se concluye que las dos partes proporcionan las mismas características de seguridad, solo que IPv6/IPsec proporciona mayores ventajas ya que IPsec se encuentra estandarizado en IPv6 y en IPv4 tiene algunos problemas de compatibilidad.

En el escenario 2 implementado con SET sobre IPv4 basa parte de su seguridad en SSL y las especificaciones de seguridad son suficientes para concluir que el protocolo IPv6 tiene características de seguridad para proporcionar una mejor autenticación y confidencialidad que SSL, es por ello que para esta parte del escenario la hipótesis se cumple.

En lo referente a SET en el escenario 2, podemos concluir que IPv6 no puede eliminar la necesidad de este mecanismo de seguridad, ya que SET se encuentra en el nivel aplicativo proporcionando seguridad a las transacciones financieras entre 3 entidades, el cliente, el comerciante y la entidad financiera, y en algunos casos una cuarta entidad, la entidad financiera emisora de la tarjeta de crédito.

Actualmente no es posible cuantificar el costo que implicaría cambiar un sitio de e_commerce a IPv6 ya que se encuentra todavía en investigación y cambiar toda la tecnología que esta sobre IPv4 llevará mucho tiempo y un costo importante. El cambio a IPv6 implica un cambio tecnológico importante, cambio en su estructura, cambio en telecomunicaciones, cambio en hardware, cambio del protocolo, cambio del uso de herramientas adicionales al protocolo, y por ende implica un cambio tecnológico muy grande, actualmente no esta evaluado en proyectos de investigación el costo que implica el cambio a IPv6.

En referencia a los costos de las herramientas de seguridad evaluadas en este trabajo de investigación, se puede decir lo siguiente: para SSL se pueden encontrar versiones libres o hasta un costo de US$500.00 dependiendo de la plataforma en la que se quiera implementar, para las VPNs sobre la red pública de Internet existen versiones libres como en Windows 2000 ó FreeBSD, contemplando solo el costo de la licencia del servidor y la de los clientes, ó hasta un firewall/VPN de US$15, 000.00 por conexión sobre líneas dedicadas, y para la implementación del protocolo SET para un sitio de e_commerce existen un rango de US$30, 000.00 hasta US$100, 000.00.

IPv6 ofrece un alto estándar para transacciones seguras sobre la red, pero ningún protocolo o aplicación pueden garantizar un camino 100% seguro para transmisión de información sobre redes.

Esta tesis contribuye a las investigaciones realizadas por el departamento de Telecomunicaciones y Redes del ITESM - Campus Monterrey.

6.2 TRABAJOS FUTUROS

Evaluar varios protocolos de administración de llaves para IPv6 y proponer uno como estándar.

Cuando la evolución de la tecnología IPv6 lo permita se proponen los siguientes trabajos de investigación:

Evaluar el escenario de una VPN sobre IPv6 en la red pública de Internet implementando su seguridad comparada con una VPN sobre líneas dedicadas, analizar si la VPN sobre la red pública de Internet ofrece las mismas ventajas de seguridad y así reducir considerablemente costos por la suspensión de renta de líneas dedicadas.

Implementar SET sobre IPV6 y evaluarlo contra SET sobre IPv4, para corroborar que IPv6 y su seguridad ofrecen una mejor opción que SSL.

ANEXO A

APLICACIÓN DESARROLLADA PARA SIMULAR E_COMMERCE

Se desarrolló un pequeño sitio para simular E_Commerce, el sitio se llamó *Universidad Angel*, la finalidad de este sitio es vender cursos a estudiantes de esta universidad o estudiantes de otras universidades que tengan convenio, la dirección electrónica es: http://mainipv6.items.mx/angel/angel.html.

Las reglas del sitio se describen a continuación:

1. Para poder ingresar al sitio se deberá estar previamente registrado, la forma de obtener dicho registro es por medio de la administración de la universidad, se tiene que ser alumno inscrito o alumno de otra universidad con convenio.
2. Se tiene un control de acceso por medio de cuenta y password, cada vez que un estudiante ingrese al sitio se almacenará un registro de su acceso al sitio.
3. El alumno podrá seleccionar un curso a la vez y tendrá que ser pagado por medio de una tarjeta de crédito.
4. Una vez que el alumno haya decidido tendrá que ingresar el número clave del curso indicado a un lado del nombre del curso, deberá seleccionar que tipo de tarjeta de crédito tiene y deberá ingresar el número de tarjeta de crédito con la efectuará el pago.
5. Una vez tecleados los datos anteriores se ingresará la compra regresando los datos del curso seleccionado y un número de factura, y en ese momento habrá terminado la compra.

A continuación se muestra un ejemplo con las pantallas del curso:

Esta será la pantalla en la que los estudiantes que deseen comprar un curso deberán ingresar su nombre de usuario y password:

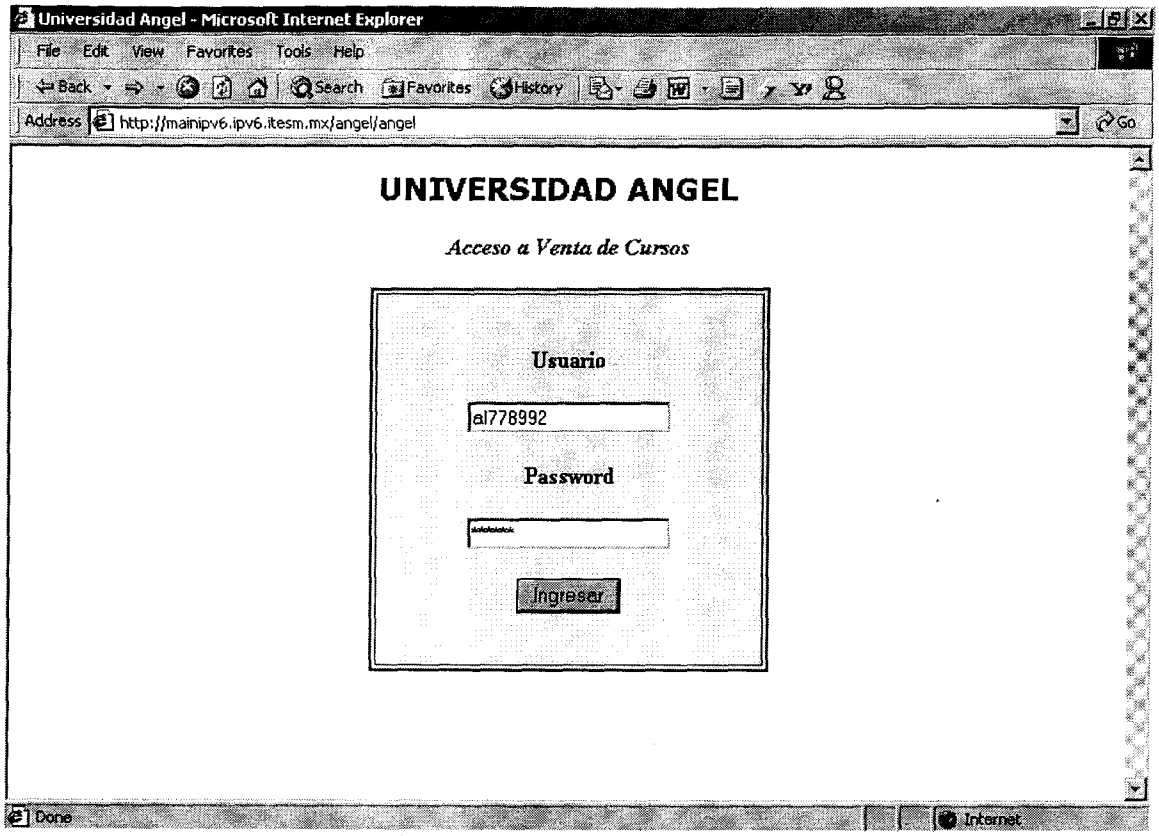


FIGURA A.1. PANTALLA DE ACCESO

Una vez que el estudiante se autentifico aparecerá una lista de los cursos disponibles con sus respectivos cursos, fecha de inicio y fecha de termino.

Más abajo aparecerá tres campos en los que deberá indicar la clave del curso que desea comprar, el tipo de tarjeta de crédito y el número de tarjeta de crédito.

Una vez tecleados los datos deberá presionar el botón comprar para ejecutar la transacción de compra.

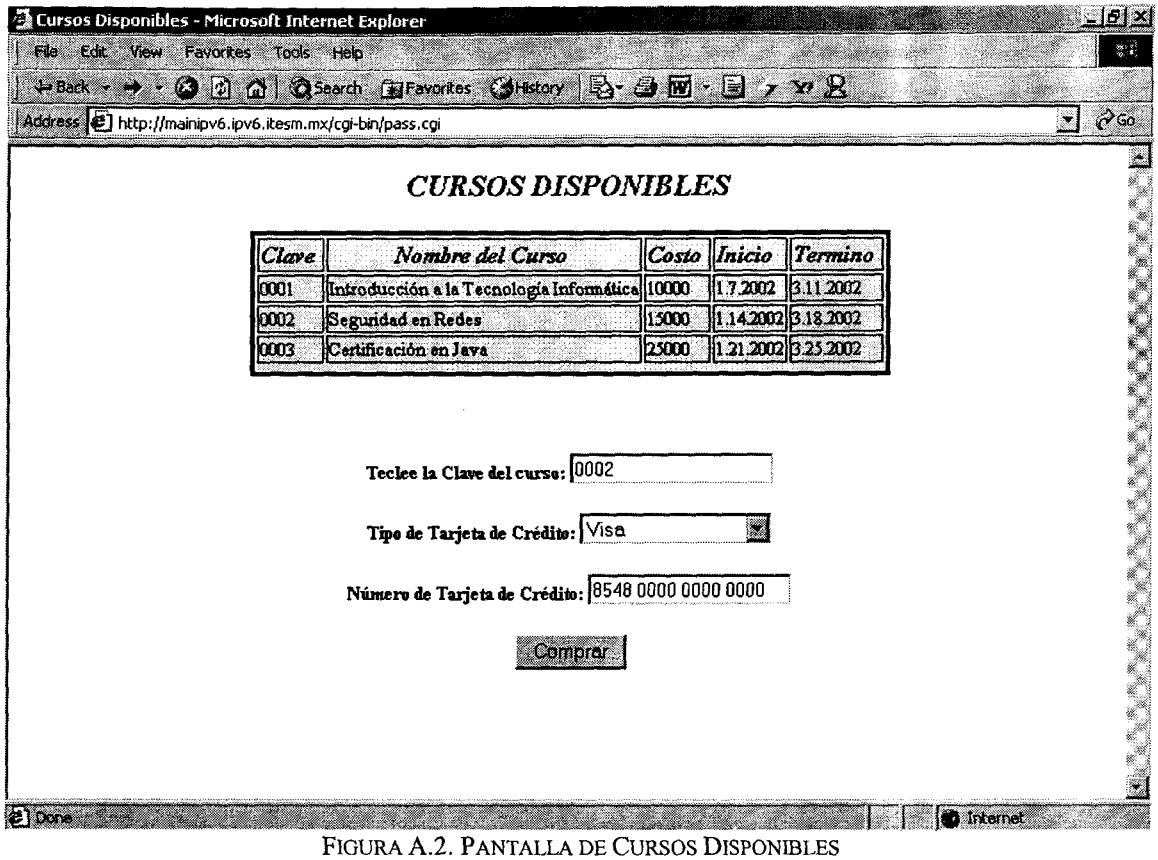


FIGURA A.2. PANTALLA DE CURSOS DISPONIBLES

Una vez que se ejecuto la transacción de compra del curso se mostrara una pantalla indicando el nombre del usuario, el curso de compro y el número de factura de la compra.

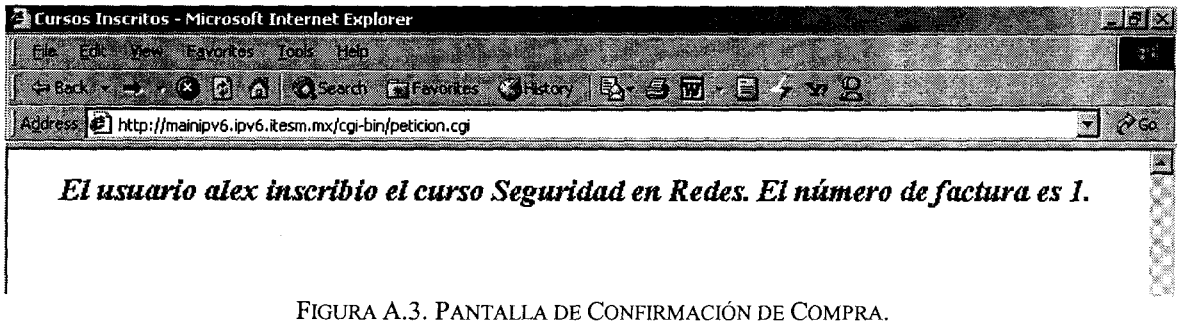


FIGURA A.3. PANTALLA DE CONFIRMACIÓN DE COMPRA.

A continuación se muestra el código fuente de la programación del sitio

El siguiente código solo muestras la ventana de control de acceso en la que él estudiante deberá ingresar su nombre de usuario y password, una vez hecho esto presionará el botón *Ingresar* y mandará llamar al programa llamado pass.cgi.

```
##########################################################################
# Angel.html: Muestra la pantalla de control de acceso y manda llamar a pass.cgi
##########################################################################

<html>
<head>
<title>Universidad Angel</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">
<p align="center"><font color="#666600" size="5" face="Verdana, Arial, Helvetica,
sans-serif"><b><font color="#000066">UNIVERISDAD
 ANGEL</font></b></font></p>
<p align="center"><i><font size="4" color="#FF0000"><b>Acceso a Venta de
Cursos</b></font></i></p>
<form name="form1" method="post" action="/cgi-bin/pass.cgi">
 <table width="37%" border="2" align="center" bgcolor="#FFFFCC"
bordercolor="#666666">
  <tr>
   <td>
    <div align="center">
     <p> </p>
     <p><b><font size="4" color="#000000">Usuario</font></b></p>
     <p>
      <input type="text" name="usuario" maxlength="10">
     </p>
     <p><b><font size="4" color="#000000">Password</font></b></p>
     <p>
      <input type="password" name="password" maxlength="15">
     </p>
     <p>
      <input type="submit" name="iniciar" value="Ingresar">
     </p>
     <p> </p>
    </div>
   </td>
  </tr>
 </table>
```

```
</form>
<p align="center"> </p>
</body>
</html>
```

El siguiente código verifica que los datos ingresados en la pantalla de control de acceso sean válidos, esto lo hace verificando los registros en el archivo *passwd*, si el usuario esta registrado le desplegará los cursos disponibles y la dará la opción de ingresar la clave del curso, el tipo de tarjeta de crédito, el número de tarjeta de crédito y le habilitara el botón que hará la petición de compra, esto lo hace llamando al cgi llamado petición.cgi.

Este código también hace el registro de cada acceso hecho a la página, almacenando un registro con el nombre del usuario, dirección IP desde la que está ingresado, la hora y la fecha.

```
#######################################################################
# Angel.html: Verifica que el usuario este registrado y despliega los cursos
# disponibles y manda llama a pecitin.cgi
#######################################################################

#!/usr/bin/perl
push (@INC, "/usr/local/apache2/cgi-bin");
require ("cgi-lib.pl");
print &PrintHeader;
&ReadParse(*regdata);

open(PASSWD, 'passwd');
@lines=<PASSWD>;
close (PASSWD);
foreach $var(@lines)
{
	@temp=split(/:/, $var);
	if ($regdata{'usuario'} eq $temp[0])
	{
		$paso=1;
		if ($regdata{'password'} eq $temp[1])
		{
			$file='accesos';
			open(Accesar,">>$file") || die "cant open acces data file\n";

			($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst)	=
localtime(time);
			$mon = $mon + 1;
```

```
                    $year = $year + 1900;

        $IP=$ENV{'REMOTE_ADDR'}.":"."$hour.$min.$mon.$mday.$year";
                    print (Accesar "$regdata{'usuario'}:$IP:\n");
                    close(Accesar);
                    break;
                }
                else
                {
                    print "PASSWORD INCORRECTO, NO PUEDE TENER
ACCESO";
                    die;
                }
        }
}
if ($paso != 1)
{
        print "USUARIO NO EXISTENTE";
        die;
}

print<<"EOP";
<html>
<head>
<title>Cursos Disponibles</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">
<p align="center"><b><i><font color="#0000CC" size="5">CURSOS
DISPONIBLES</font></i></b></p>
<table border="3" align="center" bgcolor="#FFFFCC" bordercolor="#000099">
 <tr>
  <td>
   <div align="center"><i><b><font size="4">Clave</font></b></i></div>
  </td>
  <td>
   <div align="center"><i><b><font size="4">Nombre del
Curso</font></b></i></div>
  </td>
  <td><i><b><font size="4">Costo</font></b></i></td>
  <td><i><b><font size="4">Inicio</font></b></i></td>
  <td>
   <div align="center"><i><b><font size="4">Termino</font></b></i></div>
  </td>
 </tr>
```

```
EOP
$file='cursos';
open (Curso, $file) || die "cant open cursos data file\n";
@cur=<Curso>;
close(Curso);
foreach $var(@cur)
{
        @temp=split(/:/, $var);
        print<<"EOP";
        <tr>
                <td>$temp[0]</td>
                <td>$temp[1]</td>
                <td>$temp[2]</td>
                <td>$temp[3]</td>
                <td>$temp[4]</td>
        </tr>
EOP
}

print<<"EOP";
</table>
<p> </p><form name="form1" method="post" action="/cgi-bin/peticion.cgi">
 <input type="hidden" name="usuario" value=$regdata{'usuario'}>
  <center>
  <p    align="center"><b><font    color="#000000">Teclee    la    Clave    del
curso:</font></b>
   <input type="text" name="curso" maxlength="4">
  </p>
  <p    align="center"><b><font    color="#000000">Tipo    de    Tarjeta    de
Cr&eacute;dito:</font><font color="#0000CC"></font></b>
<select name="tipo">
     <option selected>American Express</option>
     <option>MasterCard</option>
     <option>Visa</option>
   </select>
  </p>
  <p  align="center"><b><font  color="#000000">N&uacute;mero  de  Tarjeta  de
Cr&eacute;dito:</font></b>
<input type="text" name="numero" maxlength="20">
  </p>
  <p align="center">
   <input type="submit" name="comprar" value="Comprar">
  </p>
  </center>
</form>
</body>
```

```
</html>
EOP
```

El siguiente código muestra al cliente un mensaje de confirmación, además de sus funciones de almacenamiento de cursos inscritos y el pago hecho.

Para fines de la tesis se asume que se hizo una verificación con una entidad bancaria y que se autorizo el monto de la compra, por lo tanto siempre será exitosa la compra.

```
##########################################################################
# Petición.cgi: Simula que se hizo la verificación en el banco y almacena el
# curso comprado y el registro de la compra.
##########################################################################

#!/usr/bin/perl
push (@INC, "/usr/local/apache2/cgi-bin");
require ("cgi-lib.pl");
print &PrintHeader;
&ReadParse(*regdata);

$file='cursos';
open(Curso, $file)|| die "cant open cursos data file\n";
@cur=<Curso>;
close(Curso);
foreach $var(@cur)
{
	@temp=split(/:/, $var);
	if ($regdata{'curso'} eq $temp[0])
	{
		$encontrado=1;
		$costo=$temp[2];
		$nom_cur=$temp[1];
	}
}
if ($encontrado != 1)
{
	print "C U R S O   N O   E N CO N T R A D O";
	die;
}
$file='pagos';
open(Pago, ">>$file")|| die "cant open acces data file\n";

$factura=1;
```

```
# AQUI SE DEBE PEDIR LA PETICION AL BANCO Y NOS DE EL NUMERO DE
REFERENCIA DE LA AUTORIZACION
$referencia=1;

print                                                    (Pago
"$factura:$regdata{'numero'}:$costo:$referencia:$regdata{'usuario'}:\n");
close (Pago);

$file='inscritos';
open(Inscrito,">>$file")|| die "cant open cursos data file\n";
print (Inscrito "$regdata{'usuario'}:$regdata{'curso'}:$factura:\n");
close (Inscrito);

print<<"EOF";
<html>
<head>
<title>Cursos Inscritos</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">
<p align="center"><b><i><font color="#0000CC" size="5">
El usuario $regdata{'usuario'} inscribió el curso $nom_cur.\n
El monto fue $.\n
El número de factura es $factura.
</font>
</body>
</html>
EOF
```

ANEXO B

FUNCIONAMIENTO DE IBM SET DEMO

COMPONENTES DE LAS TRANSACCIONES SET

Cartera Electrónica de Consumo

La cartera electrónica de consumo es la versión en software de la cartera que utilizan los compradores para guardar sus tarjetas de crédito. Los compradores, también conocidos como tarjetahabientes, pueden adquirir carteras electrónicas de sus bancos de crédito, vía descarga directa de la red o en discos compactos o diskettes. Con esta cartera electrónica como una aplicación de ayuda en el browser, pueden hacer sus compras usando la seguridad y la identificación del SET en Internet. La interfaz gráfica del usuario (GUI por sus siglas en inglés) hace fácil de administrar individualmente las tarjetas de crédito y mantener la información de las transacciones.

La cartera es iniciada al tiempo en que se realiza el proceso de certificación por el banco de crédito, o durante el proceso de compra por el vendedor cuando el tarjetahabiendte está listo para hacer la compra. Si el tarjetahabiente quiere revisar sus compras, pueden iniciar la cartera desde el menú de inicio. Al entrar a la cartera, los tarjetahabientes deberán ingresar su nombre de usuario y su contraseña. Las contraseñas proveen un nivel extra de protección para ayudar a mantener seguras sus tarjetas de crédito.

La solución de IBM para la cartera electrónica de consumo es: IBM Consumer Wallet (Cartera de Consumo IBM)

La Caja Registradora Electrónica

Las funciones de la caja registradora electrónica como las de las caja registradora usada en las tiendas es la de manejar y almacenar la información de los pagos. Todas las transacciones del cliente al usar la cartera, fluyen directamente a la caja registradora electrónica del vendedor. La caja registradora electrónica acepta los pagos del tarjetahabiente vía Internet y pasa la información

hacia las instituciones financieras para su aprobación.

La solución de IBM para la caja registradora electrónica es: IBM Payment Manager (Administrador de Pagos IBM)

Autoridad Certificadora

Los certificados digitales son la base de las medidas de seguridad usadas para autentificar a los diferentes actores en el mercado del e_commerce, y proteger la información durante el intercambio. Los certificados o identificaciones digitales son intercambiados entre los vendedores, clientes y portales de pagos durante el ciclo de compras, identificando a cada una de las partes con el resto. Los certificados fungen como una identidad digital, similar a una identificación con fotografía en el mundo físico. Estos certificados son proporcionados por la Autoridad Certificadora. La autoridad certificadora utiliza una aplicación de software para manejar la aprobación, creación, administración, ruteo, decodificar y codificar, y otras actividades de validación de la certificación. La autoridad certificadora es dirigida por un banco de una manera similar a aplicar para una tarjeta de crédito.

La solución de IBM para la autoridad certificadora es: IBM Payment Registry (Registro de Pago IBM).

Portal de Pagos

Los portales de pagos representan a la institución financiera del comerciante en Internet. Actúa como el intérprete entre la comunicación del SET en Internet y el sistema de comunicación privada de las instituciones financieras. El comerciante utiliza la información de pagos recibida del tarjetahabiente para solicitar un autorización de la institución financiera a través del portal de pagos. La información es enviada a la institución financiera y la información de autorización es enviada al comerciante mediante el portal de pagos.

La solución de IBM para el portal de pagos es: IBM Payment Gateway (Portal de Pagos IBM).

INTERACCION DE LOS COMPONENTES

Unión de todos los actores y componentes de software: el tarjetahabiente

con la Cartera de Consumo IBM, el vendedor con el Administrador de pagos IBM, el procesador de tarjetas de crédito con el Portal de Pagos IBM, y los bancos con el Registro de Pagos IBM.

Cada pieza tiene su propio y definido papel en un proceso que es similar al hacer una compra en el mundo físico. El proceso de dos pasos que todos los involucrados deben seguir: (1) Obtener su "identificación digital" única y (2) Usar la identificación para realizar compras. A continuación, un escenario simple y resumido de como interactúan los componentes:

Obtener Identificaciones Digitales

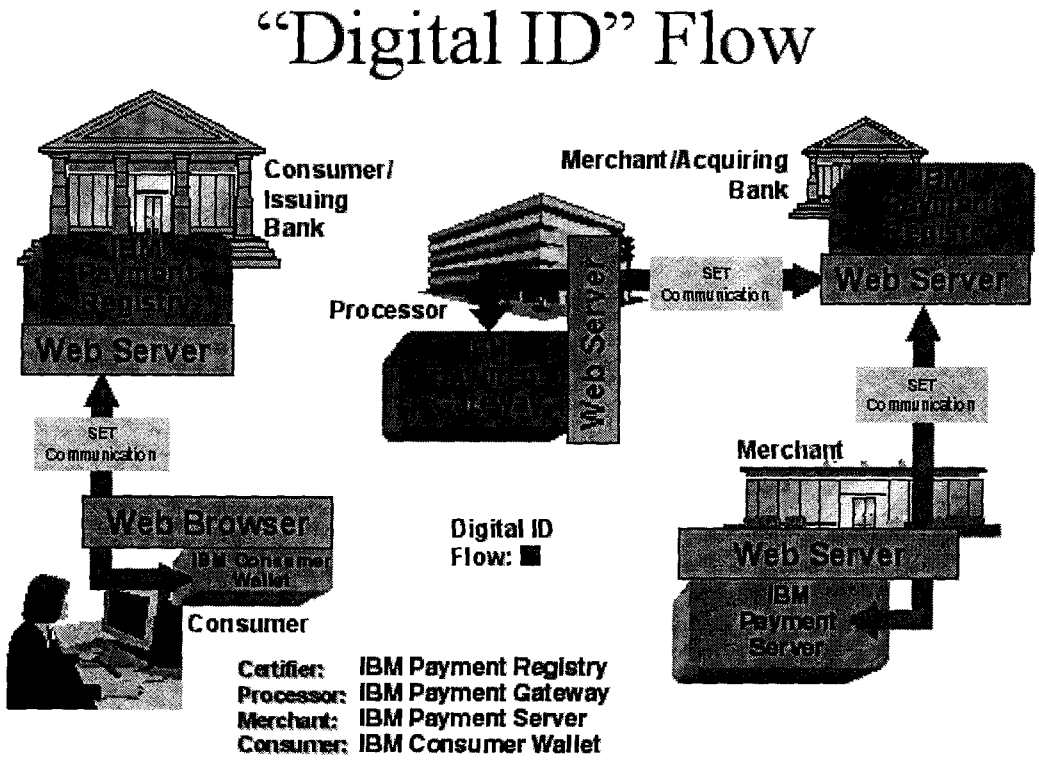


FIGURA B.1 OBTENCIÓN DE IDENTIFICACIONES DIGITALES

- El tarjetahabiente, el vendedor y el procesador de tarjetas, usan su software (Cartera de Consumo IBM, Administrador de Pagos IBM, Portal de Pagos IBM) para generar su par de llaves públicas y privadas preparándose para solicitar las identificaciones digitales.
- Cada una provee su banco (Registro de Pagos IBM como su autoridad certificadora), con su llave pública junto con información especial de identificación. Usando la Información especial de identificación, el banco evalúa cada solicitud para su autentificación.

- El Banco después expide y entrega las identificaciones digitales (certificados SET) usando el Registro de Pagos IBM.
- La Cartera de Consumo IBM, Administrador de Pagos IBM y el Portal de Pagos IBM son usados para instalar su identificación digital en preparación para su uso.

Comprar con SET

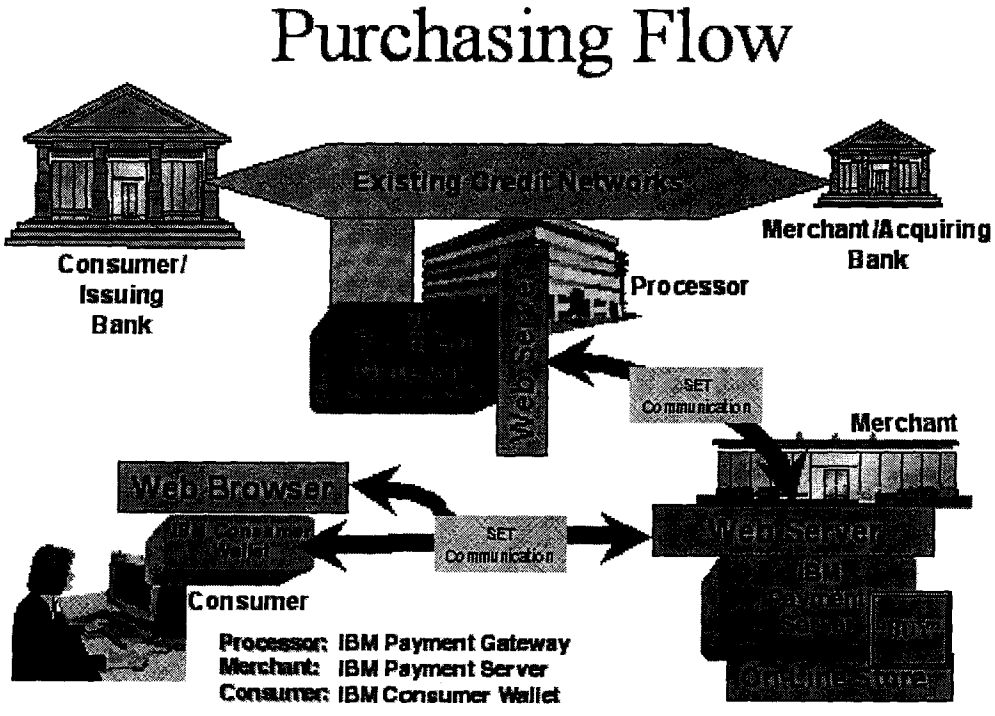


FIGURA B.2 COMPRAR CON SET

- La experiencia de la compra electrónica comienza cuando el consumidor ha seleccionado un artículo a comprar en una tienda en línea, y le son ofrecidas las opciones de pago del vendedor. Con el software Cartera de Consumo IBM instalado conteniendo la identificación digital del comprador en su PC, el consumidor da un click en el botón de opción de compra a crédito del vendedor.
- El Administrador de Pagos IBM del vendedor intercepta la requisición y regresa un mensaje de aviso al navegador del consumidor, diciendo que inicie la Cartera de Consumo IBM del consumidor. El administrador de pagos también envía a la Cartera de Consumo IBM los detalles de las compras solicitadas.
- La Cartera del Consumido IBM automáticamente abre una ventana por separado.

- El consumidor ingresa su identificación única y su clave y revisa los detalles de la compra propuesta.
- Después de verificar la información de la propuesta de compra, el consumidor hace un click en "Aceptar".
- La Cartera de Consumo IBM solicita después la identificación digital del vendedor y del procesador del Administrador de Pagos IBM del vendedor y muestra la identificación del vendedor para su verificación.
- Después de verificar y aprobar la Identificación del vendedor, el consumidor de nuevo hace un click en "Aceptar" para proceder.
- La cartera después envía un mensaje al Administrador de Pagos IBM conteniendo dos paquetes de información: la información de requisición de compra digitalmente "firmada" para el vendedor y la información de la tarjeta de crédito del comprador cifrada con la identificación del Portal de Pagos IBM, de manera que sólo el Portal pueda leerla.
- El Administrador de Pagos IBM envía la información de crédito del consumidor junto con su propia solicitud de aprobación para la tarjeta de crédito al Portal de Pagos IBM. El portal descifra la información del crédito y solicita la aprobación de la compra del consumidor al banco.
- El Portal de Pagos IBM encripta la respuesta del banco, enviándola de regreso al Administrador de Pagos IBM, aprobando o rechazando la solicitud de autorización.
- Con la aprobación, el Administrador de Pagos IBM notifica al software (de cumplimiento) del vendedor para que entregue y transmita el estatus de la orden y la información final de la compra a la Cartera de Consumo IBM.
- La Cartera de Consumo IBM recibe el mensaje de "aprobado" o "rechazado". Con la aprobación, la Cartera también recibe la información final de la compra o "recibo electrónico", almacenándolo en la base de datos de las compras del cliente para futura referencia.
- Automáticamente la Cartera de Consumo IBM se cierra y el comprador regresa al sitio del vendedor para continuar navegando en la red.
- Después, el consumidor puede abrir la Cartera de Consumo IBM y revisar el recibo.

ANEXO C

CONFIGURACIÓN DE LA VPN

C.1 CONFIGURACIÓN DEL SERVIDOR

Para la configuración del servidor VPN se utilizo el siguiente equipo y se habilitaron los siguientes servicios:

Características	Servicios
Computadora Intel Pentium III de 1 GHz de velocidad, Disco duro de 30 GB, memoria RAM de 256 MB, Sistema Operativo Windows 2000 Server, con service pack 2 y soporte para Encripción muy Fuerte(128-bit)	Servidor de Acceso Remoto de VPN Servidor de Páginas Web Servidor de FTP Servidor de Archivos Servidor de Dominio Autoridad Certificadora (CA)

TABLA C.1.1 CARACTERÍSTICAS DEL SERVIDOR VPN

Asignación de un Dominio al servidor con nombre de dominio **medusa.mty.itesm.mx** con la siguiente dirección IP 131.178.21.42 e indicar la interfaz por la que se conecta a Internet.

Selección de los siguientes protocolos de comunicación TCP/IP, IPX y NetBEUI, y del servidor de DHCP para asignarle las direcciones a sus clientes de VPN de forma dinámica. El servidor de VPN queda habilitado tanto para conexiones de acceso remoto vía LAN o por Acceso telefónico.

Descripción de las políticas de seguridad para los usuarios dados de alta en el sistema o dominio. Únicamente se habilitaron a dos usuarios como clientes de los servicios disponibles en el Servidor, el Administrador e Invitado.

Servicio	Políticas de Seguridad
Acceso Remoto	Se requiere Autentificación Solo usuarios Autorizados La contraseña no caduca Tipo de Tunel (PPTP y L2TP)
Paginas Web	Se requiere Autentificación (IIS) No se requiere Autentificación (Apache) Solo usuarios autorizados La contraseña no caduca
Ftp	No se permiten accesos Anónimos Se requiere Autentificación Solo usuario autorizados
Archivo	Se requiere Autentificación Solo usuarios Autorizados No caduca la contraseña

TABLA C.1.2. POLÍTICAS DE SEGURIDAD EN EL SERVIDOR VPN

Dependiendo del tipo de Protocolo que se desee utilizar para la comunicación con el cliente de VPN se procede a su configuración. El Servidor de VPN habilita 128 puertos para conexiones PPTP y 128 para conexiones L2TP.

Point to Point Tunneling Protocol utiliza el protocolo Point to Point the Microsoft para la autentificación de usuarios y el protocolo de Encripción Point-toPoint también de Microsoft para encapsular y encriptar el tráfico IP, IPX y NetBEUI. Se utiliza el Protocolo de Microsoft Challenge Handshake version 2 (MS-CHAP v2) para passwords fuertes asegurando de esta manera un conexión segura de VPN. Antes de establecer la conexión se solicita el nombre de usuario y su password para que sea autentificado, bajo este esquema no se requiere de una Autoridad Certificadora.

Layer Two Tunneling Protocol con IPSec utiliza el protocolo Point to Point para la autentificación de usuarios y el protocolo IPSec para encriptar y encapsular el trafico IP, IPX y NetBEUI. Esta combinación utiliza la autentificación de la identidad de la computadora basada en el uso de Certificados, para crear una asociación de seguridad entre los protocolos PPP e IPSec.

C.2 CONFIGURACIÓN DEL CLIENTE

El cliente se configuró en una computadora Laptop con las siguientes características:

Windows 2000 Profesional
Dirección dinámica
Toshiba Satellite 1735
Procesaro Intel Celeron a 700 Mhz.
64 MB en Ram y 10 GB en disco duro.

La configuración se realiza a través de Conexiones de Red y de Acceso telefónico en el panel de control, se establece una nueva conexión y se le indica que la conexión es mediante VPN, después se configura el nombre o dirección IP del Servidor de VPN y dependiendo si es a través de una intranet o por Internet será la manera de accesar al servidor si la conexión es a través de un proveedor de servicios de Internet primero se establece la conexión con este mediante la autenticación del usuario con su nombre y contraseña y luego se establece el túnel hacia el servidor.

En las siguientes figuras se muestran las características de las conexiones realizadas con el Protocolo PPTP y L2TP con el servidor medusa.mty.itesm.mx

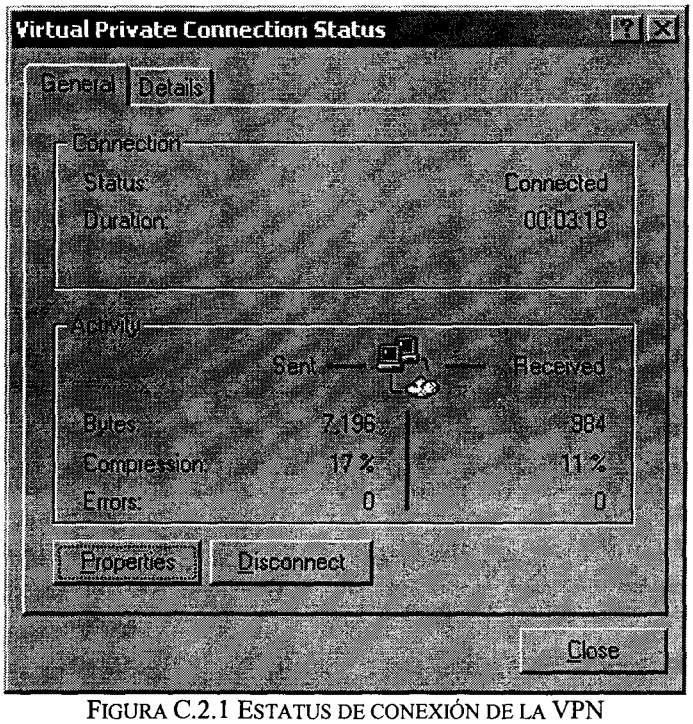


FIGURA C.2.1 ESTATUS DE CONEXIÓN DE LA VPN

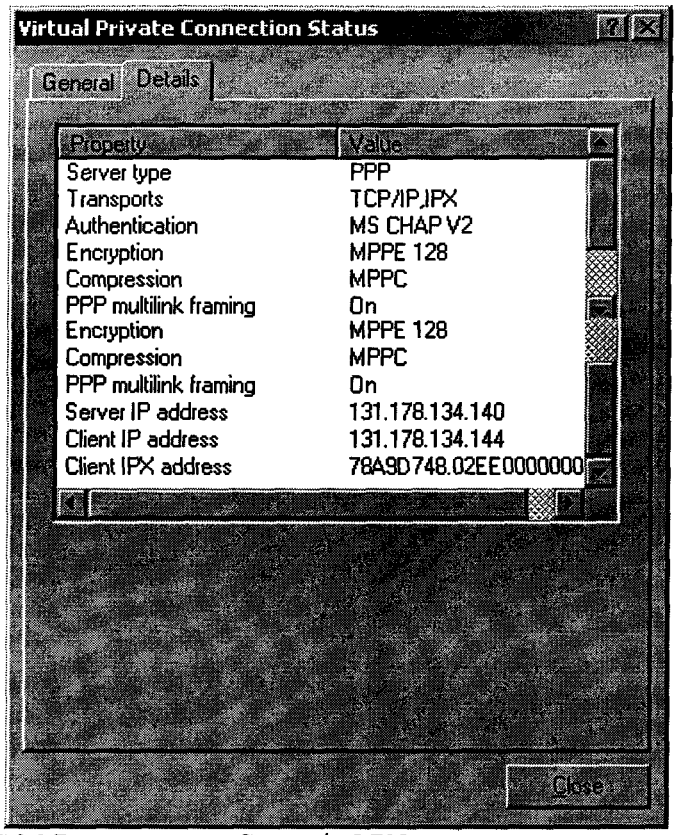


FIGURA C.2.2 DETALLES DE LA CONEXIÓN VPN UTILIZANDO EL PROTOCOLO PPTP

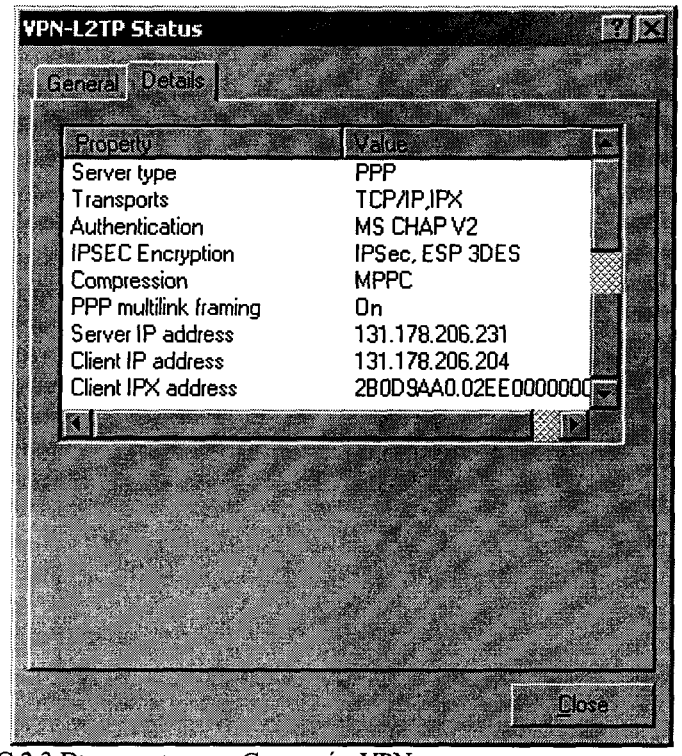


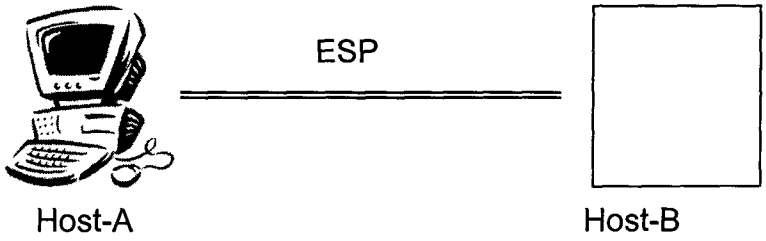
FIGURA C.2.3 DETALLES DE LA CONEXIÓN VPN UTILIZANDO EL PROTOCOLO L2TP

ANEXO D

CONFIGURACIÓN DE SEGURIDAD EN IPv6

D.1 CONFIGURACIÓN DEL MODO DE TRANSPORTE CON IPV6

ESP en modo de transporte entre Host-A y Host-B. Para la configuración de este modo solo se requieren dos hosts



Los hosts deberán tener el sistema operativo FreeBSD 4.x y el proyecto kame instalado.

La seguridad es en un solo sentido; una sesión de comunicación entre dos hosts tendrá normalmente dos asociaciones de seguridad.

Dirección Host-A a Host-B tiene las siguiente características:

SPI (Security Parameter Index)	10001
AH Algoritmo	MD5
AH Modo del algoritmo	Keyed
AH Transformada	RFC 1828
AH Llave	128 bits
AH Modo	Todo el datagrama
ESP Algoritmo	3DES
ESP Modo del algoritmo	CBC
ESP Transformada	RFC 2451
ESP Llave	192 bits
ESP Modo	Transporte

TABLA D.1.1 CARACTERÍSTICAS DE LA CONFIGURACIÓN DEL HOST-A AL HOST-B

Dirección Host-B a Host-A tiene las siguiente características:

SPI (Security Parameter Index)	10002
AH Algoritmo	MD5
AH Modo del algoritmo	Keyed
AH Transformada	RFC 1828
AH Llave	128 bits
AH Modo	Todo el datagrama
ESP Algoritmo	3DES
ESP Modo del algoritmo	CBC
ESP Transformada	RFC 2451
ESP Llave	192 bits
ESP Modo	Transporte

TABLA D.1.2 CARACTERÍSTICAS DE LA CONFIGURACIÓN DEL HOST-B AL HOST-A

El algoritmo de encripción es el *3des-cbc* siendo su llave "kamakamekamakamekamakame", su algoritmo de autenticación es *keyed-md5* siendo su llave "this is the test".

Configuración del Host-A:

Es importante que se cambie al siguiente directorio, ya que si se ejecuta el comando *setkey* marcará un error de parser debido a que tratará de reconocer direcciones de IPv4 y las que se configuran son direcciones IPv6:

```
# cd /usr/local/v6/sbin/
```

Las siguientes líneas limpian todo el estado de la información, asegurando que *setkey* tendrá un estado limpio si es re-invocado con los mismo parámetros. ^D es lo equivalente a presionar la tecla Ctrl y la letra D del teclado:

```
# setkey -c
flush;
spdflush;
^D
```

A continuación se hace la configuración del modo de transporte con la características descritas en la tabla D.1.1, *any* significa que la información que viaje de cualquiera de los puertos entre los dos hosts viajara en modo de transporte:

```
# setkey -c <<EOF
spdadd 3ffe:8241::210:4bff:fe27:2048[any] 3ffe:8241::248:54ff:fec0:b87[any] tcp -P
out ipsec esp/transport/3ffe:8241::210:4bff:fe27:2048-
3ffe:8241::248:54ff:fec0:b87/use ;
spdadd 3ffe:8241::248:54ff:fec0:b87[any] 3ffe:8241::210:4bff:fe27:2048[any] tcp -P
in ipsec esp/transport/3ffe:8241::248:54ff:fec0:b87-
3ffe:8241::210:4bff:fe27:2048/use ;
add 3ffe:8241::210:4bff:fe27:2048 3ffe:8241::248:54ff:fec0:b87
esp 0x10001
-m transport
-E 3des-cbc "kamekamekamekamekamekame"
-A keyed-md5 "this is the test" ;
add 3ffe:8241::248:54ff:fec0:b87 3ffe:8241::210:4bff:fe27:2048
esp 0x10002
-m transport
-E 3des-cbc "kamekamekamekamekamekame"
-A keyed-md5 "this is the test" ;
EOF
```

Configuración del Host-B:

Posicionarse en el siguiente directorio para que el comando *setkey* reconozca direcciones IPv6:

```
# cd /usr/local/v6/sbin/
```

Las siguientes líneas limpian todo el estado de la información, asegurando que *setkey* tendrá un estado limpio si es re-invocado con los mismo parámetros. ^D es lo equivalente a presionar la tecla Ctrl y la letra D del teclado:

```
# setkey -c
flush;
spdflush;
^D
```

A continuación se hace la configuración del modo de transporte con la características descritas en la tabla D.1.2, *any* significa que la información que viaje de cualquiera de los puertos entre los dos hosts viajara en modo de transporte:

```
# setkey -c <<EOF
spdadd 3ffe:8241::248:54ff:fec0:b87[any] 3ffe:8241::210:4bff:fe27:2048[any] tcp -P
out ipsec esp/transport/3ffe:8241::248:54ff:fec0:b87-
3ffe:8241::210:4bff:fe27:2048/use ;
spdadd 3ffe:8241::210:4bff:fe27:2048[any] 3ffe:8241::248:54ff:fec0:b87[any] tcp -P
in ipsec esp/transport/3ffe:8241::210:4bff:fe27:2048-
3ffe:8241::248:54ff:fec0:b87/use ;
add 3ffe:8241::210:4bff:fe27:2048 3ffe:8241::248:54ff:fec0:b87
esp 0x10001
-m transport
-E 3des-cbc "kamekamekamekamekamekame"
-A keyed-md5 "this is the test" ;
add 3ffe:8241::248:54ff:fec0:b87 3ffe:8241::210:4bff:fe27:2048
esp 0x10002
-m transport
-E 3des-cbc "kamekamekamekamekamekame"
-A keyed-md5 "this is the test" ;
EOF
```

D.2 CONFIGURACIÓN DEL PROYECTO TAHI

El proyecto consta de dos paquetes, la herramienta de prueba de adaptabilidad de IPv6 (v6eval) y el paquete de prueba de adaptabilidad de IPv6 (ct).

V6eval es una herramienta que puede generar y verificar cabeceras entre las que destacan para fines de la tesis, la cabecera de autenticación (AH) y la cabecera de encapsulado de carga de seguridad (ESP) de IPv6.

Ct es el programa de prueba de adaptabilidad de IPv6. Las pruebas se ejecutan en la herramienta de adaptabilidad de IPv6 (v6eval).

Ambos paquetes se obtuvieron de la dirección electrónica siguiente: http://www.tahi.org/

El procedimiento seguido para la instalación es el siguiente:

Se instalo la herramienta de prueba de adaptabilidad de IPv6 (v6eval) del proyecto TAHI en un host que tiene el sistema operativo FreeBSD, teniendo algunos problemas en la instalación, por lo cual se hizo el contacto por correo electrónico con el responsable del proyecto, quien dio algunas recomendaciones.

Se decidió formatear la máquina e instalar la versión más reciente del sistema operativo FreeBSD, la 4.4, entre uno de los requisitos para la instalación está la instalación del proyecto KAME, el cual fue instalado, kame-20011015-freebsd44-snap.

El proyecto TAHI requiere de dos hosts para ejecutar las pruebas con las mismas características mencionadas en el párrafo anterior, por lo cual se consiguió otro host para completar el laboratorio, los dos hosts se encuentran configurados con el sistema operativo FreeBSD 4.4 y el proyecto KAME-20011015 sobre IPv6.

Una vez preparados los hosts, se prosiguió a la instalación de la herramienta de prueba de adaptabilidad (v6eval) en uno de los hosts como lo requiere el proyecto, logrando con éxito la instalación de la herramienta sin los problemas surgidos en la primera instalación.

Para completar el laboratorio se hizo la instalación del paquete de prueba de adaptabilidad de IPv6 (ct), el cual aparentemente se instalo con éxito, pero al momento de ejecutar las pruebas fallaron todas.

Se volvió hacer contacto con el representante del proyecto TAHI, el cual recomendó la instalación de la nueva versión liberada recientemente, la versión instalada fue la 1.2 y la recomendada es la 1.3.

Se procedió a la instalación de la siguiente versión (1.3), algunos pasos con respecto a la versión anterior cambiaron, los cuales disiparon las dudas acumuladas en la instalación anterior, la instalación de la herramienta de prueba de adaptabilidad de IPv6 y el paquete de prueba de adaptabilidad de IPv6 resultó exitosa.

Se corrieron las pruebas del paquete de adaptabilidad de IPv6 del proyecto, con una duración aproximada de 10 horas.

El equipo principal utilizado para la implementación de este escenario es el siguiente:

- *broker.ipv6.itesm.mx*

  Características:

  FreeBSD 4.4
  3ffe:8241::40
  131.178.107.207
  Servidor Web Apache2 (IPv4/IPv6)

- *ipsec.ipv6.itesm.mx*

  Características:

  FreeBSD 4.4
  3ffe:8241::210:4bff:fe27:2048
  131.178.107.204
  Servidor Web Apache2 (IPv4/IPv6)

A continuación se hace una referencia breve de los pasos seguido para la instalación de la herramienta *V6eval*:

1. Extraer el paquete:

   % cd $SOMEWHERE
   % tar zxvf v6eval-1.3.tar.gz

2. Compilación e instalación de la herramienta:

   % cd $SOMEWHERE
   % make
   # make install

   Hacer los dispositivos especiales bpf:

   # cd /dev
   # ./MAKEDEV bpf1 bpf2 bpf3 bpf4 bpf5 bpf6 bpf7

A continuación se hace una referencia breve de los pasos seguido para la instalación del paquete *ct:*

Equipo 1:

1. Extraer el paquete:

   % tar zxvf ct-1.3.tar.gz

2. Instalación:

   % cd ct-1.3
   % su
   # make install

3. Conectar los dos equipos por el puerto COM1 con un cable Null-Módem.

Equipo 2:

4. /etc/rc.conf

   Agregar las siguiente líneas:

   ipv6_eanble="YES"
   ipv6_network="xl0"
   ipv6_default_interface="xl0"

5. /etc/ttys

   Agregar la siguiente línea:

   cuaa0 "/usr/libexec/getty std.9600" vt100 on secure

6. Configuración del Kernel:

   /usr/src/sys/i386/conf/GENERIC

   Agregar las siguientes líneas:

   options IPSEC
   options IPSEC_ESP

   # cd /usr/src/sys/i386/conf/
   # /usr/sbin/config GENERIC
   # cd ../../compile/GENERIC/
   # make depend
   # make
   # make install

Equipo 1:

7. Copiar el ejemplo disponible en el paquete:

   # cd /usr/local/v6eval/etc/
   # cp tn.def.sample tn.def

   Modificar la conexión especifica de la Mac, para este caso xl0:

   Link0 xl0

8. Copiar el ejemplo del equipo 2:

   # cp nut.def.sample nut.def

   Modificar la conexión especifica de la Mac y la dirección MAC del equipo 2, para este caso xl0 y su MAC correspondiente:

   Link0 xl0 00:90:27:14:ce:da

9. Comando cu:

   # touch /var/log/aculog
   # chmod a+rw /var/log/aculog

10. Correr las pruebas:

    % cd $SOMEWHERE/ct
    % make clean
    % make test

Para mayor detalle se puede encontrar dos archivos con la configuración detallada, INSTALL.v6eval e INSTALL.ct, dentro de los archivos del paquete una vez descomprimidos.

Debido a la falta de información técnica los resultados obtenidos fueron fallidos.

Los resultados proporcionados por el proyecto TAHI están disponibles en www.tahi.org.

ANEXO E

HERRAMIENTA DE DETECCIÓN DE RIESGOS Y VULNERABILIDADES Y HERRAMIENTA DE ATAQUE EXTERNO (SNIFFER)

E.1 NETRECON. HERRAMIENTA DE DETECCIÓN DE RIESGOS Y VULNERABILIDADES.

NetRecon es una de las mejores herramientas que existen en el mercado para la detección e identificación de Vulnerabilidades de una Red, este clasifica las vulnerabilidades según el riesgo que estas representan para el sistema. El análisis lo hace a través de una evaluación externa de la seguridad de la red que analiza y explora los sistemas de la red tratando de identificar los posibles agujeros de seguridad que hacen vulnerable al sistema. NetRecon reconstruye las escenas comunes de las intrusiones o los ataques y las reporta, al mismo tiempo que sugiere acciones correctivas.

Elimina las vulnerabilidades comunes de seguridad antes que un intruso tenga la oportunidad de atacar con el fin de garantizar los e-business de una organización.

Características principales

- Evalúa las vulnerabilidades de la red.
- Analiza múltiples Sistemas Operativos .
- Muestra el progreso del análisis en tiempo real.

Maneja tres niveles de Evaluación

- Exhaustivo (HeavyScan)

  Obtiene acceso a través de Login Server.
  Encuentra passwords encriptados usando diccionarios pequeños.
  Toma ventaja de los nombres de usuarios y passwords identificados para accesar los recursos de la red.
  Descubre vulnerabilidades analizando archivos.
  Este análisis incluye a los análisis medio y ligero.

- Medio (Medium Scan)

  Descubre vulnerabilidades en los siguientes protocolos NFS, NIS, FTP, HTTP SMB y SMTP.
  Descubre vulnerabilidades analizando de manera completa los puertos TCP y UDP.
  Incluye al análisis ligero

- Ligero (Light Scan)

  Indentificación de recursos en la red.
  Information de Alias.
  Identificación de Sistema Operativo y versión.
  Detección de Vulnerabilidades en Redes de Windows y SMTP.

Reporte de vulnerabilidades

NetRecon no solo descubre y reporta las vulnerabilidades, sino que las correlaciona para poner en evidencia el problema de fondo.

Brinda un análisis exhaustivo con una herramienta de análisis único de las rutas de acceso para ilustrar la secuencia exacta de las medidas adoptadas y descubrir una vulnerabilidad. A diferencia de otras herramientas que simplemente ofrecen explicaciones de los síntomas de los problemas, NetRecon brinda una interpretación sistemática de las causas de las vulnerabilidades.

A través del análisis único de las rutas de acceso de NetRecon, se puede rastrear los pasos que conducen a una vulnerabilidad brindando una oportunidad para llegar al fondo del problema. Con NetRecon, se obtienen cientos de datos sobre los síntomas del problema, llegando a la causa real del problema.

Ejemplo:

Vulnerability Name:	**NetWare startup file write access obtained**
Risk:	**95** ●
Description:	NetWare startup files (.NCF files) contain information about what utilities/services are loaded and information about security settings, such as packet signature levels. Write access to this information permits an attacker to change security settings, disable system auditing, load executables (such as backdoors) that can be used later to compromise the system again, and so forth.

Solution: Change access to indicated .NCF files to allow only authorized personnel (according to the company's security policy) to have access.

Additional Information:

Network Resource Type	Aliases	NetworkResource
red.netrecon.com	red, 10.1.8.1, 00:a0:29:42:b1:2d	NetWare, NetWare 3.12, IP host, Windows Networking resource

Requerimientos Técnicos : Windows NT 4.0 (WorStation, Server), 64 MB de memoria Ram mínimo, 40 MB de espacio en disco.

Estas son algunas de las Graficas de Resultado que genera el NetRecon en una prueba Exhaustiva.

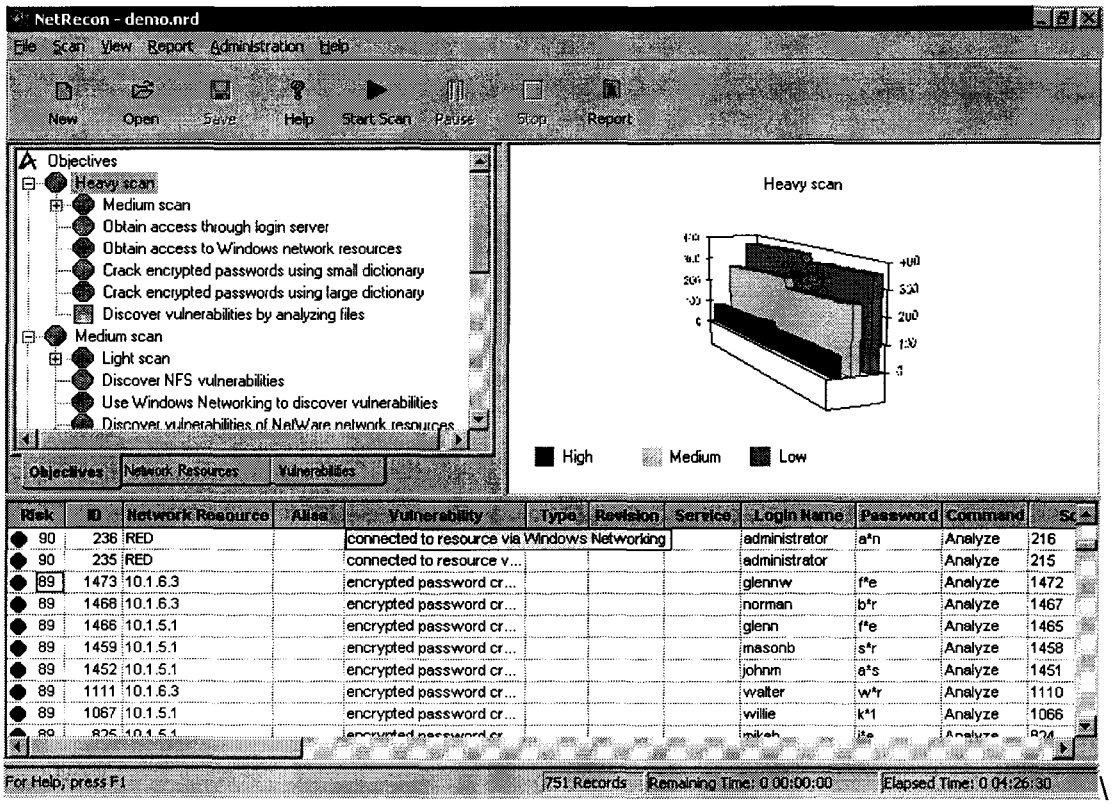


FIGURA E.1.1. EJEMPLO GRÁFICA 1 NETRECON

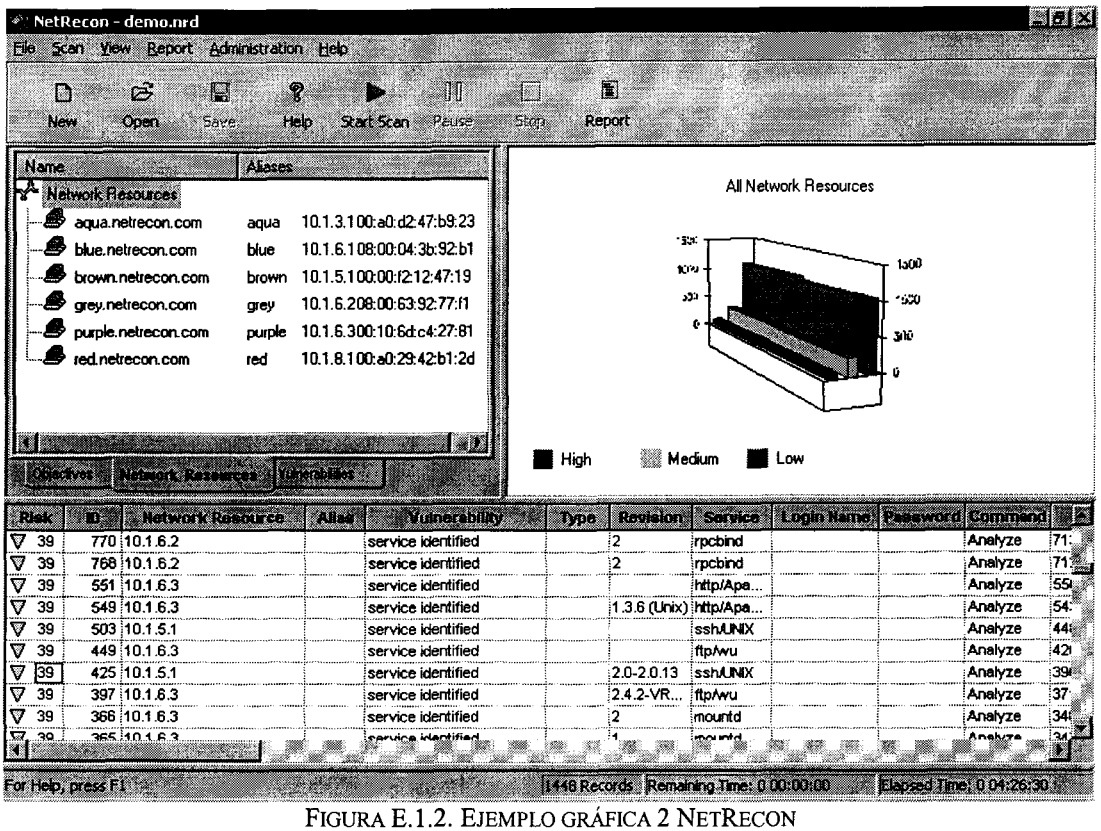


FIGURA E.1.2. EJEMPLO GRÁFICA 2 NETRECON

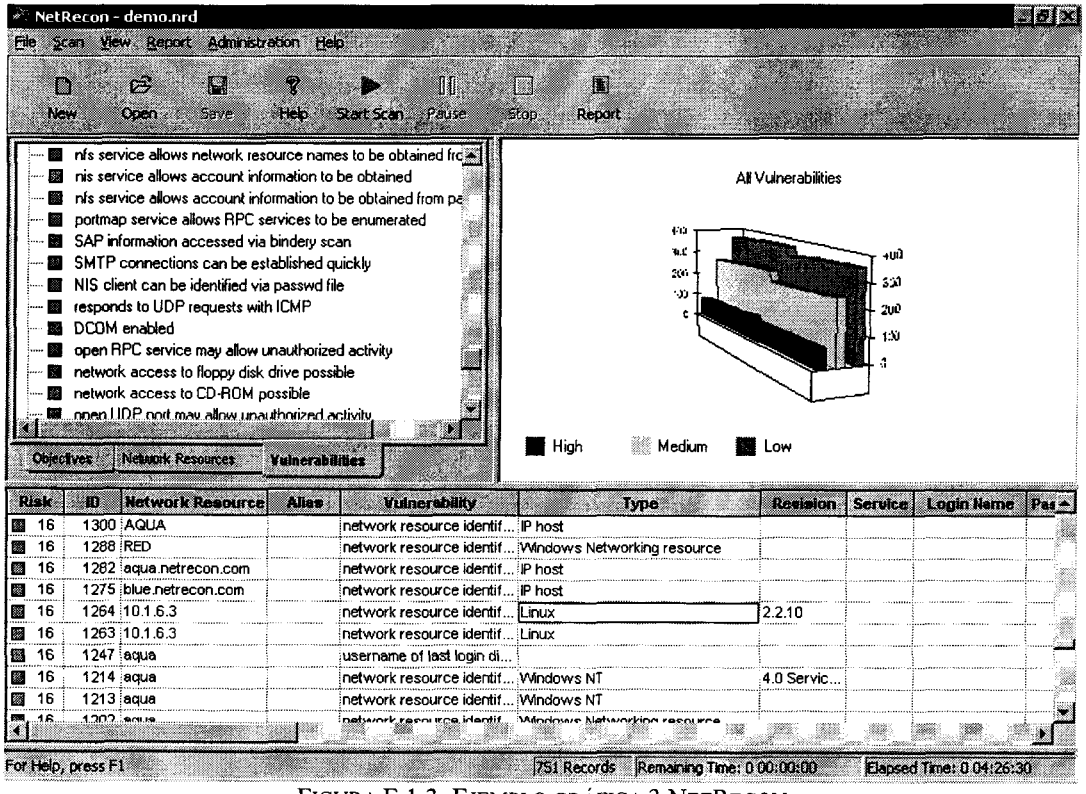


FIGURA E.1.3. EJEMPLO GRÁFICA 3 NETRECON

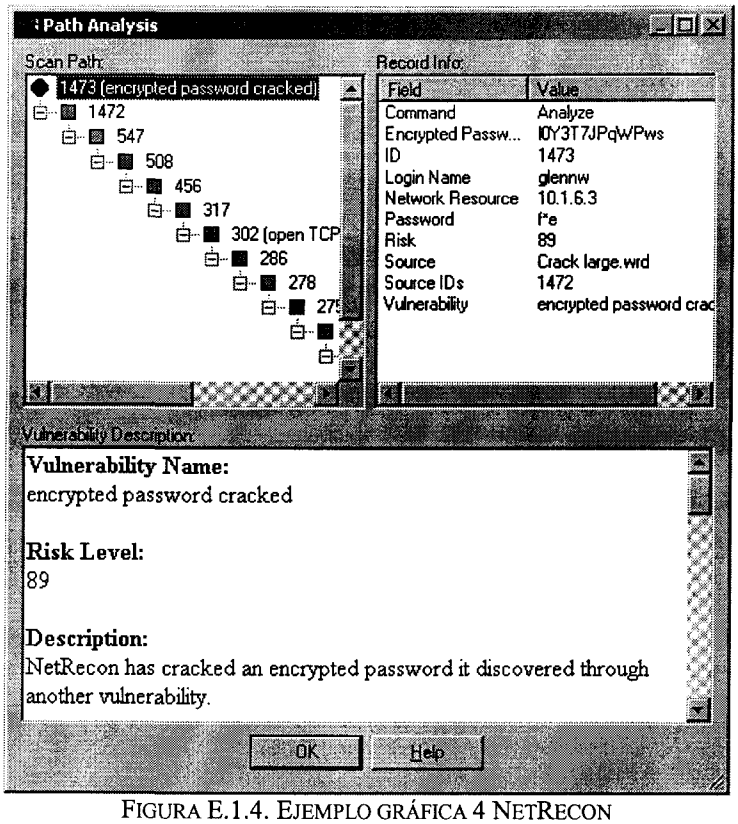


FIGURA E.1.4. EJEMPLO GRÁFICA 4 NETRECON

E.2 ETHEREAL. HERRAMIENTAS DE ATAQUE EXTERNO (SNIFFER).

Ethereal es un analizador de protocolos de Red gratuito para Unix y Windows. Permite examinar datos de una red en tiempo real o de un archivo capturado almacenado en disco. Se pueden analizar datos capturados interactivamente viendo información detallada o resumida de cada paquete.

Características:

- Ethereal tiene muchas características poderosas incluyendo un filtro de despliegue del lenguaje rico y la habilidad de ver el flujo reconstruido en una sesión de TCP.

- Ethereal puede leer archivos capturados de otras herramientas de sniffeo como: tcpdump snoop, AIX's iptrace, Microsoft's Network Monitor, Novell's LANalyzer, por mencionar algunos.

- Los datos de tiempo real pueden ser leídos sobre diversas interfases como ethernet, FDDI, PPP, token-ring, X.25, o IP sobre ATM.

- Los datos capturados pueden visualizarse vía una GUI.

- Soporta diferentes tipos interfaces y paquetes, por mencionar algunos tenemos: AFS, AH, ARP, ATM, CHAP, COPS, ESP, ETH, FDDI, FTP, IPV6, IPX, KERBEROS, L2TP, NETBIOS, PPTP por mencionar algunas.

- Las salidas pueden guardarse o imprimirse como texto en plano o PostScript®.

Algunas de las pantallas de salidas que genera son las siguientes:

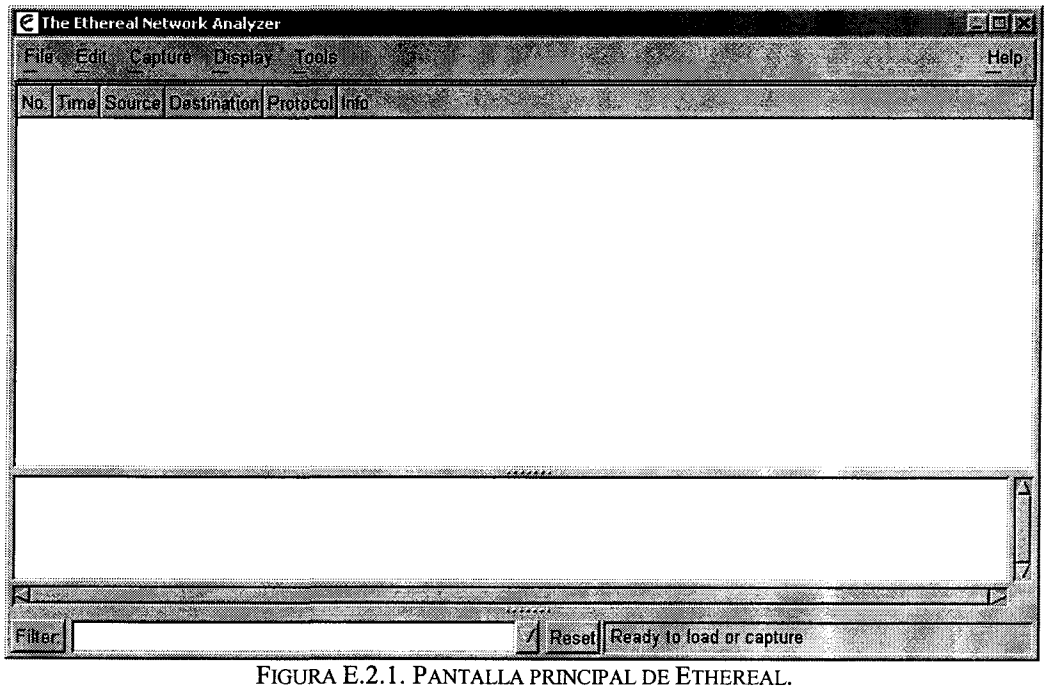


FIGURA E.2.1. PANTALLA PRINCIPAL DE ETHEREAL.

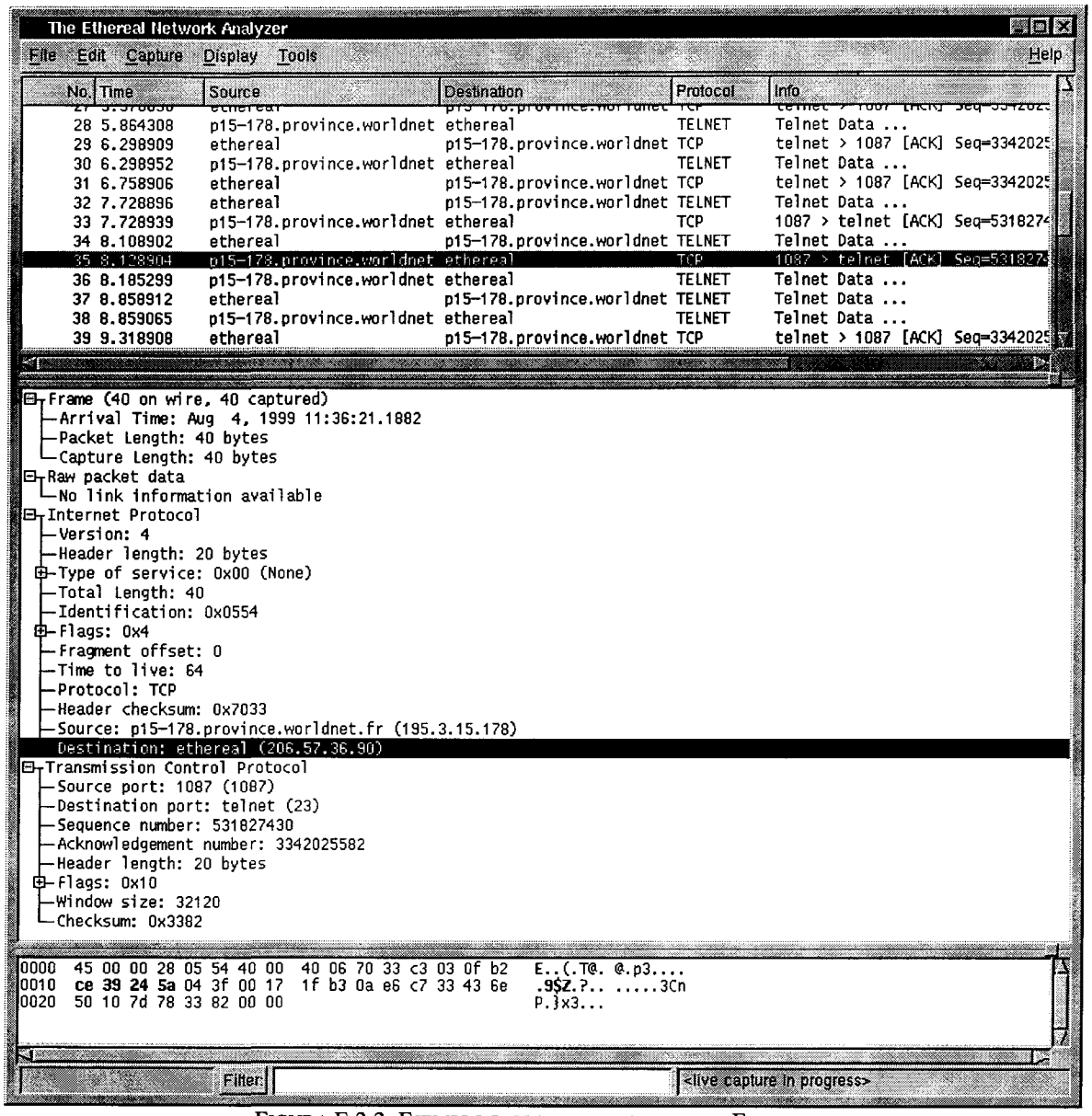


FIGURA E.2.2. EJEMPLO PANTALLA DE SALIDA DE ETHEREAL

Esta imagen se muestra el Ethereal en medio de una captura. Como se puede ver, se puede inspeccionar los datos de la captura con gran detalle, aun cuando la captura este en proceso.

The Ethereal Network Analyzer

File Edit Capture Display Tools Help

No	Len	Time	Source	Destination	Protocol	Info
1	77	0.000000	24.94.186.99	pow.zing.org	DNS (UDP)	Standard query
2	77	0.010000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
3	164	0.060000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
4	70	0.070000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
5	71	0.080000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
6	161	0.120000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
7	158	0.130000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
8	77	9.990904	24.94.186.99	pow.zing.org	DNS (UDP)	Standard query
9	77	9.990904	pow.zing.org	i.got.net	DNS (UDP)	Standard query
10	148	10.090904	i.got.net	pow.zing.org	DNS (UDP)	Standard query response
11	148	10.090904	pow.zing.org	24.94.186.99	DNS (UDP)	Standard query response

```
⊞-Frame (77 on wire, 77 captured)
⊞-Ethernet II
⊞-Internet Protocol
⊞-User Datagram Protocol
⊟-DNS query
  ├-Transaction ID: 0x83c8
  ⊞-Flags: 0x0000 (Standard query)
  ├-Questions: 1
  ├-Answer RRs: 0
  ├-Authority RRs: 0
  ├-Additional RRs: 0
  ⊟-Queries
    ⊟-www.brunching.com: type A, class inet
        Name: www.brunching.com
      ├-Type: Host address
      └-Class: inet
```

```
0000  00 50 73 2c 44 c1 08 00  20 2b 01 05 08 00 45 00   .Ps,D... .+....E.
0010  00 3f 4b e7 00 00 40 11  84 ac ce 39 24 5a cf 6f   .?K...@. ...9$Z.o
0020  e8 17 07 f4 00 35 00 2b  18 c0 83 c8 00 00 00 01   .....5.+ ........
0030  00 00 00 00 00 00 03 77  77 77 09 62 72 75 6e 63   .......w ww.brunc
0040  68 69 6e 67 03 63 6f 6d  00 00 01 00 01            hing.com .....
```

Filter: File: dns.pcap Drops: 0

FIGURA E.2.3. EJEMPLO PANTALLA DE SALIDA EN DETALLE DE ETHEREAL

Esta pantalla muestra una vista del DNS desde la perspectiva del servidor. Es interesante resaltar que el servidor demanda cuatro búsquedas para resolver el nombre, y el cliente le envío esta búsqueda antes que el servidor pudiese responder.

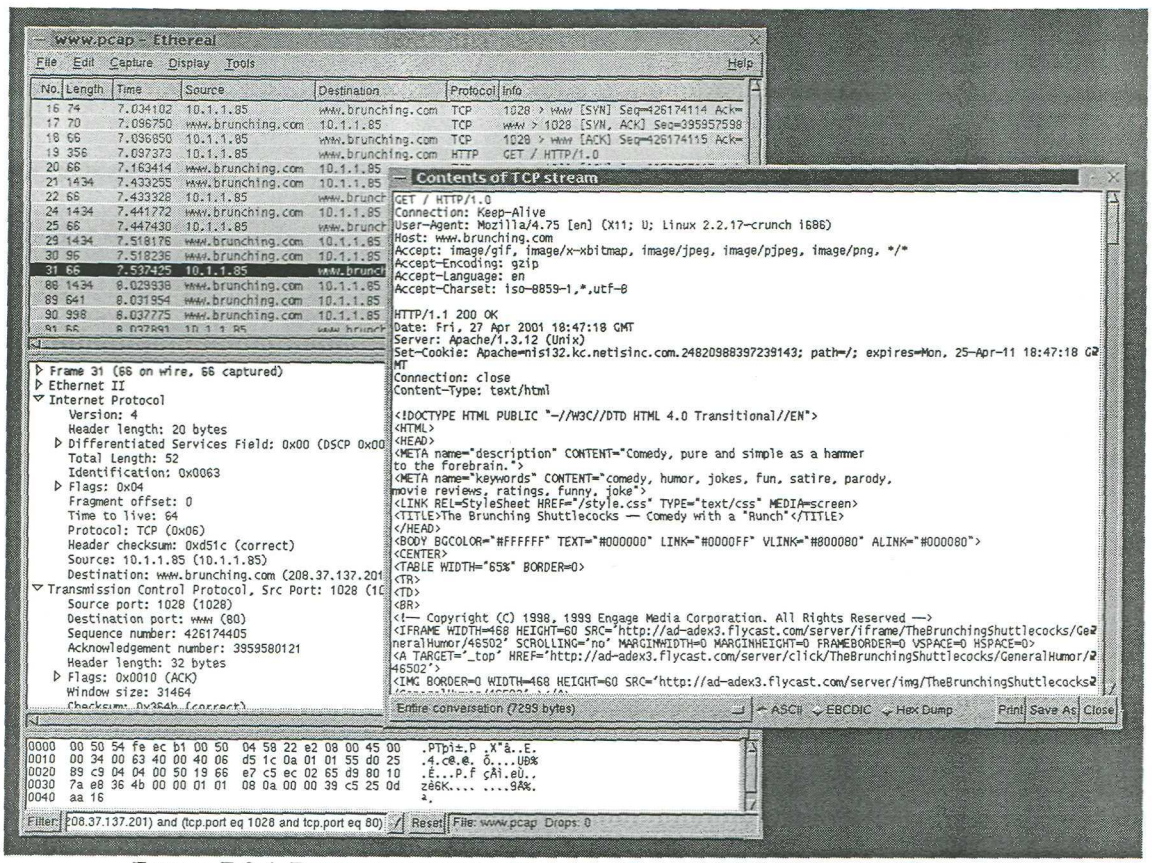


FIGURA E.2.4. EJEMPLO PANTALLA DE SALIDA FOLLOW TCP STREAM DE ETHEREAL

En esta pantalla se puede ver la opción de "Follow TCP Stream" que se encuentra en el menú "Tools", este permite inspeccionar el contenido en ASCII del los datos en el flujo TCP en una ventana separada.

Esta opción puede ser invaluable para un seguimiento de HTTP, SMTP, y problemas con las cuentas POP en el servidor.

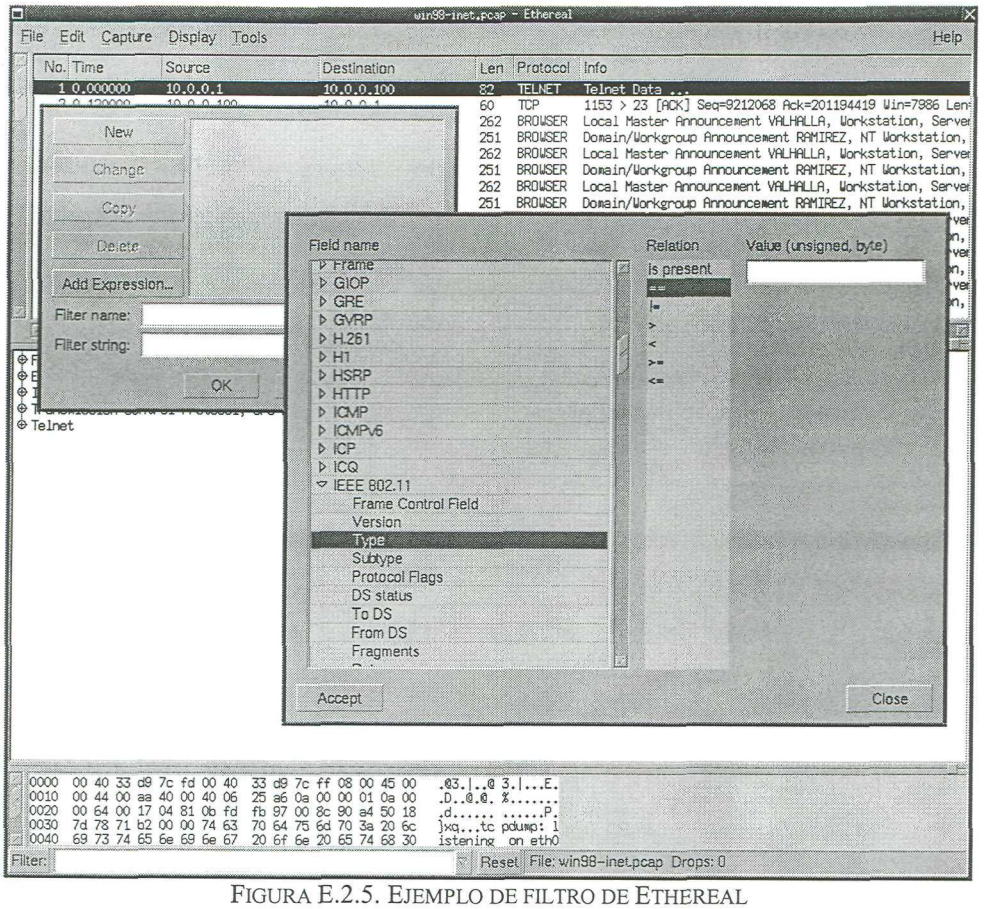


FIGURA E.2.5. EJEMPLO DE FILTRO DE ETHEREAL

La GUI de la creación del filtro permite crear filtros sobre cualquier protocolo o campo del cual Ethereal tenga conocimiento.

REFERENCIAS BIBLIOGRÁFICAS

[Bay Networks, 97] Bay Networks, The Case for IPv6; White Paper, 1997, p. 35.

[Cameron, 1999] Cameron, Debra. "Electronic Commerce. The New Business Platform for the Internet". En:
Computer Technology Research Corp., 1999.

[Comer, 96] Comer, Douglas E. "Redes globales de información con Internet y TCP/IP. Principios básicos, protocolos y arquitecturas". Tercera edición. En:
Prentice Hall, 1996.

[Forné, 2000] Forné, Jordi. "Seguridad en Internet". En:
http://www-mat.upc.es/~jforne/seguridad_internet.html, 2000.

[FreeBSD, 2001] "FreeBSD Handbook". En:
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/

[Gai, 1998] Gai, Silvano. "Internetworking IPv6 with CISCO Routers". En:
Mc Graw-Hill Series on Computer Communications, 1998.

[Garfinkel, 1997] Garfinkel, Simson with Spafford, Gene. "Web Security & Commerce". En:
O'Reilly. 1997.

[Goncalves, 99] Goncalves, Markus, Niles y Kitty. "IPv6 networks[computer file]". En:
NetLibrary, Inc.1999.

[Goralski, 99] Goralski, W. Waclawski, D. "Virtual Private Networks. Achivieving Secure Internet Commerce and Enterprisewide Communications". En:
Computer Technology Research Corp. 1999.

[Greenstein, 2000] Greenstein, Marilyn. Feinman, Todd M. "Electronic Commerce: Security, Risk Management and Control". En:
Irwin McGraw-Hill. 2000.

[Herrmann, 1996] Herrmann, Eric. "CGI Programming with Perl in a week". En:
Sams Net. 1996.

[Huitema, 98] Huitema, Christian. "IPv6 The New Internet Protocol". En:
Prentice Hall PTR, 1998.

[IBM, 2000]"IBM SET demo". En:
http://216.208.176.9/setca/setdemo.html

[IEEE Network, 98] IEEE Network. "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6". En:
IEEE Network 1998, p. 28-33

[Kame, 2001] "Kame Project". En:
www.kame.net

[Kassab] Kassab, Carlos. "Perl – Practical Extraction and Report Language". En:
http://www.glin.com.mx/perl/docs/lib/pod/perl.html

[Loshin, 99] Loshin, Pete. "Ipv6 Clearly Explained". En:
Morgan Kaufmann, 1999.

[Martín, 2000] Martín Cruz, Roberto. "IPv4 vs IPv6". En:
http://tejo.usal.es/~nines/d.alumnos/ipv6/index.html

[Miller, 2000] Miller, Mark A. "Implementing IPv6". Second Edition. En:
M&T Books, 2000.

[Miller, 98] Miller, Stewarts S. "IPV6: The Next Generation Internet Protocol". En:
Digital Press, 1998.

[Morant, 2000] Morant Ramón, José Luis, Dávila Muro, Jorge y Sancho Rodríguez, Justo. "Protección de la Información". En:
http://porsche.ls.fi.upm.es/ProtInfo/Temario/Temario_ProtInfo.htm

[Raise] RaiSe. "Sniffers". En:
UNDERSEC Security Team
http://www.undersec.com/staff/raise/sniffers.txt

[Rajput, 2000] Rajput, Wasim E. "E-Commerce Systems Architecture and Aplications". En:
Artech House Publishers, 2000.

[Salus, 2000] Salus, Peter H. "IPv6 Addressing RFCs". En:
Morgan Kaufmann, 2000.

[Silva, 2001] Silva Rubio, Renán Rafael. "Seguridad en Redes". En:
ITESM, 2001.

[Tahi, 2001] "Tahi Project". En:
www.tahi.org

[Tanenbaum, 97] Tanenbaum. "Redes de computadoras", Tercera edición. En:
Pearson, 1997.

[Villalón, 2000] Villalón Huerta, Antonio. "Seguridad en Unix y Redes". En:
http://lucas.hispalinux.es/Manuales-LuCAS/SEGUNIX/unixsec-1.2/, 2000.

[Wall, 2000] Wall, Larry. Christiansen, Tom. Orwant Jon. "Programming Perl". Tercera edición. En:
O'REILLY, 2000.

[Zamora] Agurto Zamora, José. Perez vera, Ximena. Leiva Riffo, Pablo. "El Comercio Electrónico y la seguridad". En:
http://members.es.tripod.de/sistemacomputacion/sistemados.htm

Centro de Información-Biblioteca
3000200055438