INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

DISEÑO DE UN LABORATORIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN EN REDES DE CÓMPUTO

Trabajo que para obtener el grado de
Especialista en Seguridad Informática y
Tecnologías de la Información

P R E S E N T A

Ing. Marco Gustavo Sáenz González

Directores de Tesina: M. C. Eleazar Aguirre Anaya

Ciudad de México, Agosto 2009

SIP-14

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESINA

En la Ciudad de México, D. F. siendo las 18:00 horas del día 30 del mes de octubre del 2009 se reunieron los miembros de la Comisión Revisora de Tesina designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULH. para examinar la tesina titulada:

"Diseño de un Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en Redes de Cómputo"

Presentada por el alumno:

Sáenz	**González**	**Marco Gustavo**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

B	0	8	1	6	7	5

aspirante de:

ESPECIALIDAD EN SEGURIDAD INFORMÁTICA Y TECNOLOGÍAS DE LA INFORMACIÓN

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESINA***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director de tesina

M. en C. Eleazar Aguirre Anaya

Co-Director de tesina

Dr. Héctor Manuel Pérez Meana

M. en C. Marcos Arturo Rosales García

INSTITUTO POLITÉCNICO NACIONAL
ESTADOS UNIDOS MEXICANOS
S.E.P.
SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION
ESIME CULHUACAN

EL PRESIDENTE DEL COLEGIO

Dr. Héctor Manuel Pérez Meana

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México el día 17 del mes Noviembre del año 2009, el que suscribe Marco Gustavo Sáenz González alumno del Programa de Especialización en Seguridad Informática y Tecnologías de la Información con número de registro B081675, adscrito a SEPI-ESIME CULHUACAN , manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección de M. en C. Eleazar Aguirre Anaya y cede los derechos del trabajo intitulado "Diseño de un Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en Redes de Cómputo, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección mgsaenzg@mail.sedena.gob.mx. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Marco Gustavo Sáenz González

Nombre y firma

AGRADEZCO A MIS PADRES QUE ME DIERON UNA EDUCACIÓN INTEGRAL

A MI HERMANA QUE ME HA APOYADO EN CADA UNA DE LAS ETAPAS DE MI VIDA

A MI HERMANO QUIEN ME APOYO EN MOMENTOS DIFÍCILES

A MIS HIJOS QUE ME TIENEN EL CARIÑO Y LA PACIENCIA AUN CUANDO LES HE QUITADO HORAS DE CONVIVENCIA

A MI ESPOSA QUIEN ES UN PILAR EN MI VIDA

Y GRACIAS A DIOS POR LA SALUD Y VIDA

ÍNDICE GENERAL

CAPÍTULO 1
REDES (TCP/IP, 802.3, 802.11) Y VULNERABILIDADES GENÉRICAS

CAPÍTULO 2
ESTÁNDARES Y NORMAS APLICABLES A LAS PRUEBAS DE SEGURIDAD

CAPÍTULO 3

DISEÑO DE UN ESQUEMA GENERAL DE UN LABORATORIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN.

CAPÍTULO 4

MARCO LEGAL

CAPÍTULO 5

PROPUESTA DE IMPLEMENTACIÓN DEL LABORATORIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

RESUMEN

La presente Tesina propone el diseño de un Laboratorio donde se realicen análisis y pruebas a la seguridad en redes de cómputo para su implementación en organizaciones tipo Institución o de manera independiente.

Este Laboratorio puede operar de manera fija en una organización o separarse en módulos por medio de equipos de cómputo móviles, los cuales cuentan con diferentes herramientas de análisis de seguridad para su operación independiente.

Como parte final, los resultados que se obtengan deben proporcionar la información necesaria para proponer mecanismos de seguridad que disminuyan los riesgos de robo, pérdida, alteración o daño de los activos (información, hardware, software, equipo, personal e instalaciones) en redes de cómputo.

ABSTRACT

This Thesis intends to design a Laboratory where computer network security analysis and tests can take place for its use on Institutions or independent organizations.

This Laboratory can operate firmly in an organization or separate in modules through mobile computer equipment, which include different security analysis for its independent operation.

As a final report, the results obtained have to propose the necessary information to intend security mechanisms that will decrease stealing risks, loss, alteration or damage to the assets (information, hardware, software, equipment, personal or installations) on computer networks.

INTRODUCCIÓN

Los sistemas de información y las redes de cómputo presentan un avance tecnológico y crecimiento constante, lo que hace que sean cada vez más complejos proporcionando servicios y aplicaciones con el fin de atender a las necesidades de un mundo globalizado y tendiente al desarrollo de las Tecnologías de la Información (TI). Este desarrollo lleva consigo fallas y deficiencias en la seguridad de las TI que ponen en riesgos de los recursos, personal, instalaciones e información de las Organizaciones.

Es por eso que se plantea crear un área técnica especializada en analizar y realizar pruebas a la seguridad en redes de cómputo y se proporcionen propuestas de solución a las fallas detectadas con el fin de disminuir las vulnerabilidades, riesgos y amenazas a las que están expuestas dichas redes.

I. DELIMITACIÓN DEL TEMA

Se plantea la creación de un Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en Redes de Cómputo por medio del diseño de un área técnica especializada en detectar, verificar y comprobar deficiencias de seguridad informática.

Los trabajos del diseño se limitan a proponer el esquema general del laboratorio, sus funciones y los procesos generales para el desarrollo de los análisis y pruebas de la seguridad en redes de cómputo IEEE 802.3 ya que es el estándar de redes de cómputo de área loca más común.

El desarrollo de la presente Tesina está basado principalmente en el Manual de la Metodología Abierta de Testeo de la Seguridad (OSSTMM de ISECOM) por ser un manual disponible al público fundamentado en estándares internacionales como el NIST (National Institute of Standards and Technology) y contempla leyes internacionales y nacionales con el fin de prevenir al analista de delitos o problemas de tipo legal, mercantil o administrativo en la ejecución de las pruebas.

II. OBJETIVOS

Diseñar un Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en redes de cómputo.

OBJETIVOS PARTICULARES

1. Analizar el funcionamiento de pila de protocolos TCP/IP y redes IEEE 802.3 con el fin de detectar sus vulnerabilidades.

2. Proponer un estándar de análisis y pruebas de la seguridad informática.

3. Proponer el esquema general y funcionamiento de un laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en redes de cómputo, describiendo sus funciones y procesos generales.

III. JUSTIFICACIÓN

Con el diseño de un Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en redes de cómputo se puede implementar un área técnica especializada capaz de detectar fallas de seguridad con el fin de proponer mecanismos de seguridad que aminoren dichas deficiencias. Con ello reducir los riesgos de robo, pérdida o alteración de la información y cualquier otro daño a los activos de la Organización.

CAPITULO 1

REDES (TCP/IP, 802.3, 802.11) Y VULNERABILIDADES GENÉRICAS

1.1 INTRODUCCIÓN

Con el crecimiento constante de las redes de datos y en especial de Internet, la protección de los activos de las Instituciones tanto de gobierno como del Sector Privado, que para este caso se le nombrarán solo como **Organizaciones**, no solo ha sido un factor importante en el desempeño de estas, sino que ha evolucionado como un factor crítico y primordial para la supervivencia en un entorno globalizado.

Según el CERT (Computer Emergency Response Team), en diciembre de 1994 se recibieron 29,580 correos electrónicos y 3,664 llamadas reportando incidentes de seguridad en cómputo de los cuales de destacan:

1. Ataques por “sniffer”
2. Ataques vía correo electrónico.
3. Ataques a sistemas de archivos de red.
4. Ataques a los servicios de red.

Para enero del 2003 se recibieron 542,754 mensajes de correo reportando incidentes de seguridad informática, registrando 3,784 reporte de vulnerabilidades.

Otro dato importante es que del 70 al 80% de los ataques a las redes de cómputo y sus activos provienen del interior de las mismas, siendo estos tipos de ataques los más dañinos y con mayor impacto para las Organizaciones.

También es necesario identificar como parte de la problemática a los usuarios que por desconocimiento de los sistemas utilizados pueden ser causantes fallas de seguridad que tienen como consecuencia robo, pérdida o fuga de información, así como de los demás activos de la red o de la Organización.

Según los reportes de **"CSI Computer Crime & Security Survey 2008",** este año se basaron en los resultados la respuestas de 522 profesionales de la seguridad en cómputo de corporaciones de Estados Unidos de América como agencias de gobierno, instituciones financieras, instituciones médicas y universidades como se muestra en la tabla 1.1-1

Tipo de incidente	2004	2005	2006	2007	2008
Denegación de servicio	39%	32%	25%	25%	21%
Robo de Laptop	49%	48%	47%	50%	42%
Fraude de telecomunicaciones	10%	10%	8%	5%	5%
Accesos no autorizados	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Fraudes Financieros	8%	7%	9%	12%	12%
Abusos de Información Privilegiada	59%	48%	42%	59%	44%
Penetración de Sistemas	17%	14%	15%	13%	13%
Sabotaje	5%	2%	3%	4%	2%
Robo o pérdida de información privada	10%	9%	9%	8%	9%
Desde dispositivos móviles					4%
Desde otros recursos					5%
Abuso de redes inalámbricas	15%	16%	14%	17%	14%
Alteración de páginas Web	7%	5%	6%	10%	6%
Uso indebido de aplicaciones Web	10%	5%	6%	9%	11%
Bots				21%	20%
Ataques DNS				6%	8%
Abuso de mensajes instantáneos				25%	21%
Password Sniffing				10%	9%
Robo o pérdida de datos de clientes				17%	17%
Desde dispositivos móviles					8%
Desde otros dispositivos					8%

Tabla No.1.1-1 Reporte de "CSI Computer Crime & Security Survey 2008"

1.2 REDES IEEE 802.3

IEEE Standard for Information Technology, IEEE Std. 802.3-2005, New York December 2005.

Las redes LAN de alta velocidad están basadas en tecnología Ethernet y el IEEE 802.3 describe las especificaciones técnicas de las cuales incluye 3 principales categorías:

1. Ethernet son especificaciones de operación a 10 Mbps sobre cable coaxial.

2. 100 Mbps Ethernet o “Fast Ethernet” con velocidades de operación a 100 Mbps sobre cable par trenzado en cobre.

3. 1000 Mbps Ethernet o mejor conocido como “Gigabit Ethernet” con velocidades de operación de 1000 Mbps sobre fibra óptica y cable par trenzado en cobre.

Emplea como método de acceso a la red “**CSMA/CD”** Método de acceso múltiple al medio con detección de portadora y detección de colisiones (***Carrier Sense Multiple Acces with Collision Detection***) este método funciona básicamente de la siguiente manera:

1. Si el medio se encuentra libre, transmite; en otro caso se aplica el siguiente paso.

2. Si el medio se encuentra ocupado, continúa escuchando hasta que el canal se libere, en cuyo caso transmite inmediatamente.

3. Si se detecta una colisión durante la transmisión, se transmite una pequeña señal de interferencia para asegurarse de que todas las estaciones constaten la colisión. A continuación, se deja de transmitir.

4. Tras la emisión de la señal de interferencia, la estación espera una cantidad aleatoria de tiempo conocida como espera **(*backoff*),** intentando transmitir de nuevo a continuación volviendo al primer paso. Otro de los puntos que nos ayudarán a entender los diferentes ataques que serán tratados más delante de esta Tesina, en cuanto a las redes Ethernet, los datos se transmiten por todo el canal, esto quiere decir que todas las estaciones son capaces de ver o recibir la información.

1.2.1 Formato de la trama IEEE 802.3

El formato de la trama se describe en la tabla No. 1.2.1-1 que se muestra a continuación.

Preámbulo 7 Octetos	Preámbulo
Delimitador del comienzo de trama SFD (Start Frame Delimiter) 1 Octeto	SFD
Dirección destino DA (Destination Address) 6 Octetos	DIRECCIÓN DESTINO
Dirección Origen SA (Source Address) 6 Octetos	DIRECCIÓN ORIGEN
Longitud 2 Octetos	LONGITUD/TIPO
Datos LLC >= 0	DATOS LLC
Relleno >=0	RELLENO
Secuencia de comprobación de tramas FCS (Frame Check Sequence)4 octetos	SECUENCIA DE COMPROBACIÓN

Tabla No. 1.2.1-1 Formato de la trama IEEE 802.3

Una red Ethernet tradicional es *semi-duplex,* es decir, puede transmitir una trama o recibirla pero no ambas cosas al mismo tiempo. Para poder realizar esta acción se debe contar con tarjetas adaptadoras *full-duplex,* lo cual provoca un cambio en la topología de “bus” a

topología en estrella y requiere que el concentrador sea conmutado, así cada estación constituye un dominio de colisión separado y por lo mismo no existe colisiones y el método CSMA/CD no es necesario.

1.2.2 Vulnerabilidades de Ethernet

La principal vulnerabilidad de Ethernet y 802.3 es que son redes de difusión o promiscuas, es decir, la información se transmite por todo el canal, siendo posible que otras terminales conectadas al mismo canal puedan ver las tramas enviadas.

1.3 REDES INALÁMBRICAS IEEE 802.11x)

Existen diferentes tipos de redes inalámbricas y para efecto de los casos de estudio de interés de la presente Tesina se presenta un resumen las especificadas en el estándar IEEE 802.11x.

1.3.1 Arquitectura IEEE 802.11

El componente básico de una LAN inalámbrica es un conjunto básico de servicios (BSS, Basic Service Set) consiste en un número de estaciones ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido. Un BSS puede funcionar aisladamente o bien estar conectado a un sistema troncal de distribución (DS, Distribution System) a través de un punto de acceso (AP, Access Point) que efectúa las funciones de puente. El protocolo MAC puede ser completamente distribuido o bien estar controlado por una función central de coordinación ubicada en el punto de acceso.

1.3.2 Servicios de IEEE 802.11

La normatividad de IEEE 802.11 define nueve servicios

1. Asociación
2. Autenticación

3. Fin de autenticación
4. Disociación
5. Distribución
6. Integridad de MSDU
7. Privacidad
8. Re-asociación

El proveedor de servicios puede ser tanto una estación como el DS. Los servicios de la estación son implementados en cada estación IEEE 802.3, incluyendo la estación que constituye el AP *(Access Point)*. Los servicios de distribución son proporcionados entre BSS diferentes y deben ser implementados en un AP o en cualquier otro dispositivo específico conectado al sistema de distribución.

Tres de los servicios enumerados se emplean para controlar los accesos a una LAN IEEE 802.11 y para proporcionar confidencialidad. Los seis servicios restantes dan soporte a la entrega de unidades de datos de servicio MAC *(MSDU, MAC Service Data Units)* entre estaciones. Una MSDU es un bloque de datos que el usuario MAC le pasa a la capa MAC, generalmente en forma de una PDU LLC. Si una MSDU es demasiado grande para ser transmitida en una sola trama MAC, puede ser fragmentada y transmitida en una serie de tramas.

Distribución de mensaje dentro de un DS**.** Esto implica dos servicios, la distribución y la integración. La distribución es el servicio primario utilizado por las estaciones para intercambiar tramas MAC cuando la trama debe atravesar el DS para pasar de una estación de un BSS a otra estación en un BSS diferente.

La integración permite la transferencia de datos entre una estación situada en una LAN IEEE 802.11 y otra estación en una LAN IEEE 802.x que se encuentre integrada con la primera

1.4 ANÁLISIS DEL PROTOCOLO TCP/IP POR SU NATURALEZA

En este punto se realiza un análisis de la pila de protocolos TCP/IP que por su naturaleza fue un protocolo creado para comunicación, en un principio no fue pensado en seguridad lo que representa vulnerabilidades en el protocolo y que son tema de estudio para la presente Tesina.

Como primer paso debemos ubicar las capas del protocolo TCP/IP y asociarlas al modelo OSI de ISO, esto con el fin de describir un panorama general dentro de las redes como se muestra en la figura 1.4-1.

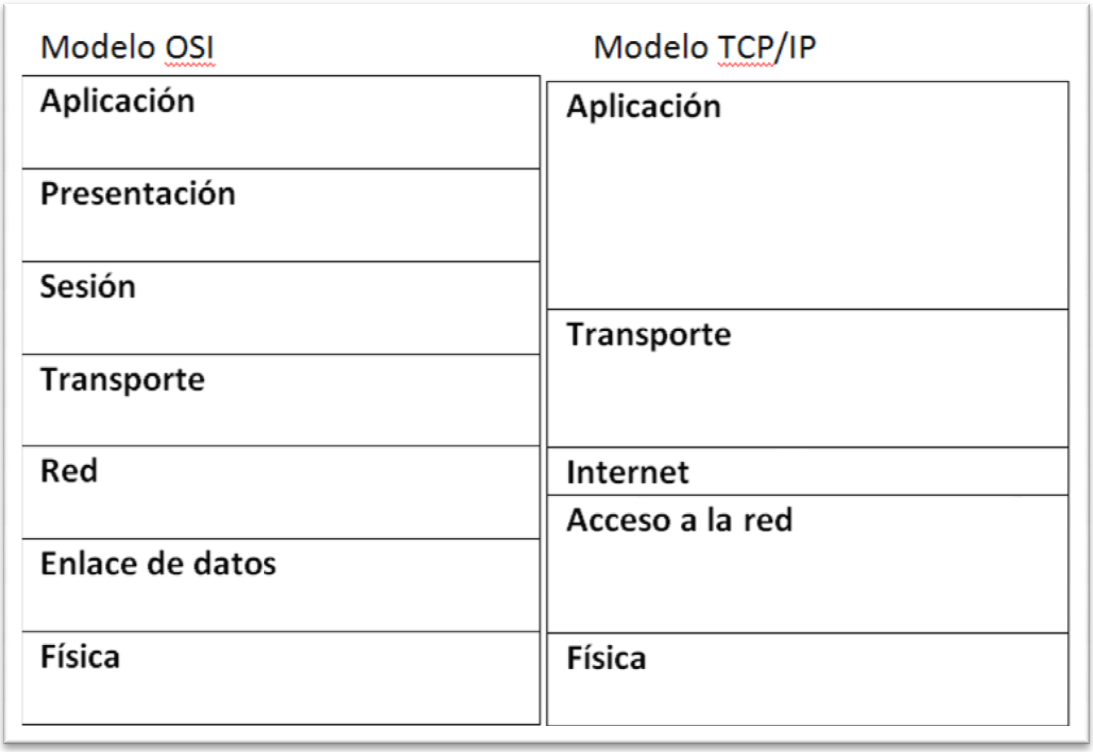

Fig. 1.4-1 Comparación del Protocolo TCP/IP y el Modelo OSI por capas.

Para fines prácticos no se describe a detalle el funcionamiento de cada una de las capas de los diferentes modelos.

En cada una de las capas de TCP/IP se observan diferentes protocolos de red que se distribuyen de acuerdo a su funcionamiento y su interacción con los demás protocolos como se muestra en la figura 1.4-2.

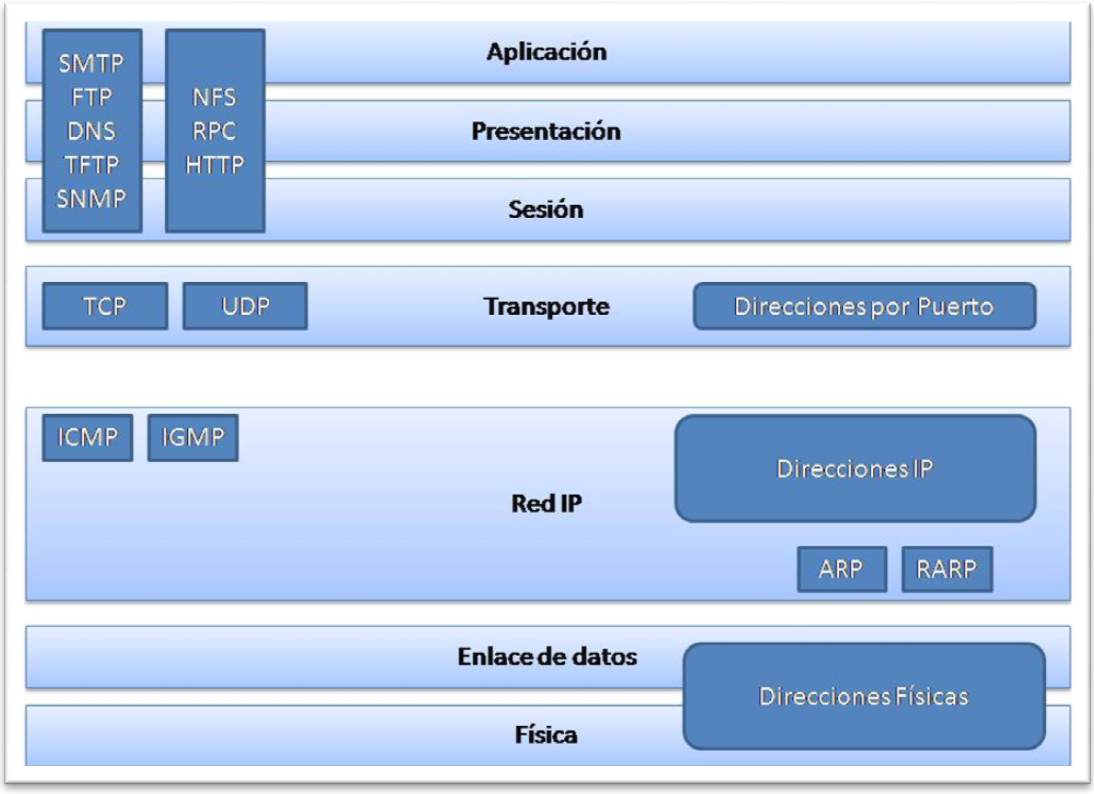

Fig. No.1.4-2 Pila de protocolos TCP/IP

En las figuras anteriores se observa cada uno de los protocolos de la pila de protocolos TCP/IP, y su interacción entre ellos.

A continuación se describen los protocolos mas comúnmente usados y con los cuales se realizan la mayoría de los ataques en las redes de cómputo.

1.4.1 Protocolo de Internet IP (*INTERNET PROTOCOL*)

IP es un estándar con especificaciones en el RFC791. Se emplea para definir direcciones virtuales para su identificación. Esto permite a los equipos conectados, aparte de tener una dirección física, contar con una dirección lógica que consta 32 bits separado en 4 octetos.

IP es el protocolo encargado de que los datos lleguen a su destino entre redes, escogiendo el camino por el cual se llevaran los paquetes de información. **Es un protocolo no confiable, ya que no asegura la recepción final en el equipo destino.**

La cabecera de la trama IP se describe en la figura 1.4.1-1 como se muestra a continuación:

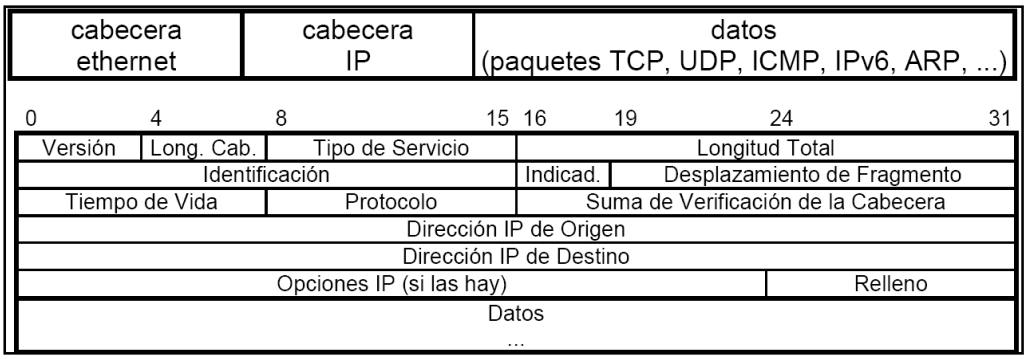

Fig. 1.4.1-1 Cabecera de la Trama IP.

Long. Cab. es la longitud de la cabecera IP en múltiplo de 32 bits.

Tipo de Servicio (TOS) Se utiliza para la prioridad de los paquetes IP

- Bits 0-2 (precedencia): Nivel de prioridad del paquete.
- Bits 3-6 (Tipo de servicio):
- Bit 8 (MBZ) no se utiliza y debe ser cero.

La longitud total en bytes del paquete incluyendo la cabecera.

Número de identificación, indicadores y desplazamiento del fragmento: Se utiliza para el seguimiento de las partes cuando un paquete se deba fragmentar.

Tiempo de vida: Es el número máximo de ruteadores a través de los que puede pasar el paquete IP. Dicho número se decrementa cada

vez que pasa por un sistema hasta que llega a cero y el paquete se destruye y se envía un paquete ICMP al origen.

Protocolo: Número que indica cual es el protocolo del paquete contenido dentro de la sección de datos del paquete IP (1=ICMP, 6=TCP, 17=UDP).

Suma de verificación de cabecera: Permite comprobar si la cabecera se daño durante el camino. No hay suma de comprobación de datos.

Dirección IP origen y Dirección IP destino.

Opciones IP: Información adicional para funciones como la seguridad y el encaminamiento (no operación, seguridad, ruta de origen, desconectada, ruta de origen estricta, registro de la ruta, identificador de flujo y marcas de tiempo).

1.4.2 Protocolo de resolución de direcciones (ARP)

El protocolo ARP, es el responsable de resolver las direcciones físicas en una red LAN y de convertir las direcciones de red a direcciones físicas o direcciones ***"Ethernet"*** de 48 bits para su transmisión sobre una red Ethernet como se explicó en el Capítulo 1.2.

Sus especificaciones se describen en el RFC 826.

Su función es simple, si una terminal desea transmitir utiliza una dirección IP, la cual para poder interactuar en una red Ethernet debe ser convertida en una dirección física que el hardware pueda reconocer y transportarla a través de la LAN.

Cuando una terminal busca en la red otra terminal, consulta las tablas ARP conocidas como "***ARP cache",*** es decir, son tablas que contienen la información de las direcciones físicas relacionadas con

sus direcciones IP respectivas y esta información se guarda durante un tiempo determinado, si la dirección buscada no se encuentra en la tabla, se envía una trama ARP, esta trama ARP, en su bloque de MAC Destino se envía un “Broadcast” FF:FF:FF:FF:FF:FF. se realiza un *“broadcast”* para anunciar la nueva dirección en un formato *“ARP request”* o *“Respuesta ARP”* y si existe una terminal con esa dirección esta manda un *“ARP replay”* de regreso la cual contiene la dirección física y dirección IP así como información de la ruta origen si es que ha pasado por algún puente. Entonces la información se guarda en el *“ARP cache”* de la terminal origen.

Cabe aclarar que el funcionamiento de ARP es diferente para ATM, el cual no se describe en este documento.

Las tablas ARP guardan la información del punto de acceso donde se segmenta o delimita la red al que se conectan los dispositivos y es el punto de acceso el que genera los paquetes ARP, asi esta dirección física y su dirección IP se guardan en las terminales. Cuando una terminal hace una petición a otra terminal, envía los paquetes a través del punto de acceso.

1.4.3 Envenenamiento y suplantación ARP *(ARP POISON Y ARP SPOOFING)*

El ataque de envenenamiento ARP consiste en el envío de paquetes ARP Request en un tiempo mínimo o por lo menos más rápido que el punto de acceso, así todas las terminales guardan en sus tablas ARP la dirección IP de las demás terminales pero asociadas a la dirección MAC del atacante, con esto la información que se envíe a las diferentes IP de la red, serán enviadas a la dirección MAC del atacante.

Este tipo de ataque funciona en redes *Ethernet* conectadas en switches o puertas de enlace (*Gateway*), es decir en equipos de conectividad que trabajen en la capa 3 del Modelo OSI de ISO.

Si el atacante no reenvía los paquetes de información, se genera una denegación de servicio, ya que los paquetes nunca llegan a su destino y por lo mismo no reciben respuesta.

Si la terminal atacante reenvía los paquetes a su destino, se genera lo que se conoce como ***"ARP Spoofing"* o Suplantación ARP.** En este tipo de ataque el usuario no percibe el ataque si no consulta sus tablas ARP.

1.4.4 Protocolo TCP

Sus especificaciones se encuentran en el RFC 793. Es el protocolo encargado de que la información se reconstruya de forma correcta mediante números de secuencia para que llegue a su destino y para pasarla a la aplicación. Es la capa que se encuentra encima del protocolo de Internet y el propósito principal es proporcionar un servicio de conexión o circuito lógico fiable y seguro entre procesos el cual requiere una serie de mecanismos relacionados con las siguientes áreas:

- Transferencia básica de datos
- Fiabilidad
- Control de flujo
- Multiplexado
- Conexiones
- Prioridad y seguridad

El formato de la cabecera del protocolo TCP se describe en la tabla 1.4.4-1 que se muestra a continuación:

16 Bits	**Puerto Origen**
16 Bits	**Puerto Destino**
32 Bits Especifica el numero de secuencia del primer byte de datos del segmento TCP	**Número de Secuencia**
32 Bits Si la bandera ACK está activo, este campo contiene el valor del siguiente número de secuencia que el sistema espera recibir.	**Número de reconocimiento**
4 Bits Indica donde finaliza la cabecera y donde comienza el campo de datos	**Data Offset**
6 Bits	**Reservado**
6 Bits Las Banderas determinan el funcionamiento de la conexión TCP	**Flags o Banderas**
16 Bits Para control de flujo de los datos	**Ventana TCP**
16 Bits Campo de comprobación de integridad	**Suma de verificación**
16 Bits Indica el desplazamiento en el campo de datos donde se encuentran los datos urgentes	**Puntero Urgente**
Variable	**Campo Opcional**
Variable. Rellenar el segmento TCP con ceros	**Padding (relleno)**

Tabla 1.4.4-1 Formato de la cabecera TCP

1.4.5 Protocolo UDP (*USER DATAGRAM PROTOCOL*)

El protocolo UDP se especifica en el RFC 768, es un protocolo de nivel de transporte basado en el intercambio de datagramas sin que se establezca una conexión, ya que el datagrama contiene suficiente información de direccionamiento en su cabecera.

El formato de la cabecera del protocolo UDP se muestra en la figura 1.4.5-1

16 Bits Opcional	**Puerto Origen**
16 Bits	**Puerto Destino**
16 Bits	**Longitud del mensaje**
16 Bits Opcional	**Suma de verificación**
Longitud variable	**Datos**

Fig. 1.4.5-1 Formato de la cabecera UDP

1.4.6 Protocolo TELNET

El protocolo Telnet se especifica en los RFC 854 y es un protocolo que se usa para interconectar terminales o dispositivos en una red.

El protocolo proporciona reglas básicas que permiten vincular a un cliente con un intérprete de comandos del lado del servidor.

Telnet se aplica sobre una conexión TCP y envía datos en formato ASCII codificados en 8 bits.

Este protocolo establece una conexión y envío de datos en claro, por lo que no emplea algún mecanismo de cifrado, haciéndolo vulnerable. Y utiliza para la comunicación el puesto 23.

El protocolo se basa en tres conceptos básicos:

1. El paradigma de terminal virtual en una red: Proporciona una interface estándar entre dispositivos y equipos de cómputo independientemente del sistema operativo o tipo de tecnología.

2. El principio de opciones negociadas: Telnet ofrece un sistema de negociación de opciones que permiten el uso de funciones avanzadas en ambos lados.

3. Las reglas de negociación:

Telnet es un protocolo base al que se le aplican otros protocolos de la pila de protocolos TCP/IP como FTP, SMTP,POP3, etc).

1.4.7 Protocolo FTP

El protocolo FTP (Protocolo de Transferencia de Archivos) tiene sus especificaciones en el RFC 959, es un protocolo como su nombre lo dice para la transmisión de archivos.

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

Los objetivos del protocolo FTP son:

1. Permitir que equipos remotos compartan archivos.

2. Permitir la independencia del sistema de archivos que puedan tener el cliente y el servidor.

3. Permitir una transferencia de archivos eficaz y confiable.

FTP es otro de los protocolos que realizan su conexión y envío de datos en claro por lo que es vulnerable al “Sniffing”.

1.4.8 Protocolo HTTP

El protocolo HTTP por sus siglas en inglés (Hyper Text Transfer Protocol) y sus especificaciones se encuentran en el RFC 2616.

HTTP es un protocolo de nivel de aplicación utilizado para distribuir y compartir información principalmente en Internet entre el cliente (a través de un navegador) y el servidor Web.

Es un protocolo basado en actividades de solicitud-respuesta y se describe en cuatro pasos principalmente:

1. El navegador abre una conexión.

2. El navegador envía una solicitud al servidor.

3. El servidor envía una respuesta al navegador.

4. La conexión se cierra.

Uno de los aspectos a considerar es que HTTP envía datos en texto claro, por lo que no emplea algún mecanismo de cifrado y utiliza por estándar el puerto 80.

CAPITULO 2
ESTÁNDARES Y NORMAS APLICABLES A LAS PRUEBAS DE LA SEGURIDAD

2.1 INTRODUCCIÓN

Actualmente existen diferentes certificados, manuales, metodologías y normas que regulen las actividades de análisis y pruebas a la seguridad en el manejo de la información. La mayoría están basados en los estándares de ISO 27001 y 27002 y documentos del INSTITUTO Nacional de Estándares y Tecnologías del Departamento de Comercio de los Estados Unidos de América (NIST). Uno de ellos es el **"Manual de la Metodología Abierta para el Testeo de la Seguridad del Instituto para la Seguridad y Metodologías Abiertas"** (*Open Source Security Methodology Manual OSSTMM de ISECOM*).

Otro documento de referencia es el **"Marco de Referencia de Evaluación de Sistemas de Seguridad de la Información"** (*ISSAF Information System Security Assessmente Framework de OISSG Open Information System Security Group*)

Para efectos de la presente Tesina, se describe a detalles el "OSSTMM", por ser este el manual de referencia para la realización de las pruebas y análisis de la seguridad por los siguientes motivos:

1. Cuenta con un sustento legal y basado en estándares internacionales y contempla el respeto a las leyes de diferentes países incluyendo las leyes mexicanas.

2. Dicho manual se encuentra al alcance del suscrito.

Así mismo se cuenta con el documento *ISSAF,* el cual solo se hace referencia y un breve resumen de dicho documento.

El documento del ISSAF cuenta con procedimientos de utilidad que sirven para el desarrollo del Laboratorio propuesto, sin embargo el documento en mención carece de sustento legal y su última actualización y revisión es de mayo del 2006, por lo que solo tomaran en cuenta aspectos relevantes para el desarrollo de la presente Tesina.

Por otra parte, en México se cuenta con diferentes leyes y reglamentos que regulan la seguridad en el manejo de la información como son:

1. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

2. Ley de Propiedad de la Industria.

3. Ley Federal de Derechos de Autor.

4. Código Penal Federal y Código Federal de Procedimientos Penales.

Las pruebas de penetración deben contemplar las leyes nacionales, internacionales, locales, reglamentos industriales y políticas de la organización. Siempre trabajando en coordinación con la organización que requiera este tipo de pruebas.

2.2 NIST (NATIONAL INSTITUTE OF STADARDS AND TECNOLOGY) GUÍA TÉCNICA DE PRUEBAS Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SP800-115)

2.2.1 INTRODUCCIÓN

El NIST, desarrolla este documento en cumplimiento de sus responsabilidades estatutarias en el marco de la Administración de Seguridad de Información Federal (FISMA 2002 Ley publicada 107-347).

2.2.2 Propósito

El propósito contar con un documento establezca las guía a seguir en una organización con el fin de que planeen, conduzcan y elaboren técnicamente su administración y pruebas de seguridad de la información, analizando y desarrollando las estrategias que ayuden a mitigar los fallos.

2.2.3 Pruebas de Seguridad y Descripción del Examen

La Evaluación de Seguridad de la Información es el proceso de determinar el grado de eficacia de la entidad que está siendo evaluada, en respuesta a objetivos de seguridad específicos.

Las Pruebas es el proceso del ejercicio uno o mas objetos de evaluación bajo condiciones específicas para comparar el comportamiento real con el esperado.

El examen es el proceso de comprobación, inspección, revisión, observación, estudio y análisis o evaluación de uno o más objetos para facilitar la comprensión y lograr la aclaración o la obtención de pruebas.

2.2.4 Metodología de evaluación de la Seguridad de la Información

Una metodología de evaluación de Seguridad de la Información ofrece una serie de ventajas. Su metodología debe contener como mínimo las siguientes fases:

1. Planeación: Se utiliza para la recolección de información necesaria para la evaluación de la ejecución, los activos que deberán ser evaluados, las amenazas a las que están expuestos y los controles de seguridad que se utilizarán para mitigar las amenazas y desarrollar un enfoque de evaluación.

2. Ejecución: Los principales objetivos para la fase de ejecución son identificar las vulnerabilidades y validarlas. Esta fase debe considerar las actividades relacionadas con el método y técnicas de evaluación. Al finalizar esta etapa, los asesores deben de haber identificado el sistema, red, organización, procesos y vulnerabilidades.

3. Post-ejecución: El periodo posterior a la fase de ejecución se centra en el análisis de las vulnerabilidades identificadas para determinar las causas y establecer las recomendaciones de mitigación y elaborara un informe final.

2.2.5 Técnicas de Evaluación

Existen diferentes técnicas de evaluación, para efectos del documento del NIST se revisan 3 técnicas:

1. Técnicas de Revisión o de Examen: Se trata de técnicas de examen utilizadas para evaluar los sistemas, aplicaciones, redes, políticas y procedimientos para detectar las vulnerabilidades y por lo regular son realizadas manualmente. Entre ellas se incluyen la documentación, registro, reglas y la configuración de los sistemas de revisión.

2. Identificación de Objetivos y Técnicas de Análisis: Este tipo de técnicas se identifican las vulnerabilidades en los sistemas, puertos, servicios, aplicaciones y son detectadas principalmente con el empleo de herramientas automatizadas.

3. Técnicas de validación de vulnerabilidades de los objetivos: Estas consisten en corroborar la existencia de las vulnerabilidades y se puede realizar manualmente o por medio de herramientas automatizadas. En esta fase incluye la validación de contraseñas, pruebas de penetración, ingeniería social y pruebas de seguridad en las aplicaciones.

2.2.6 Cuerpo del documento

En los siguientes puntos del documento del NIST, se abordan los temas donde se describen los detalles de las técnicas de examen, de identificación de los objetivos y de análisis.

Estos aspectos son tomados a detalle en el Manual de la Metodología Abierta de Testeo de la Seguridad y mismos detalles que se abordan de manera práctica durante el desarrollo del esquema que se propone en la presente Tesina en el Capítulo 3.

2.3 MANUAL DE LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD (*OSSTMM ISECOM*)

2.3.1 Introducción

Como su nombre lo dice es un manual que describe una metodología aplicable a las pruebas de la seguridad, para fines prácticos solo se describen los puntos de mayor importancia y se presentan de manera esquemática para dar al lector un panorama general de los procesos en el análisis y pruebas de la seguridad.

El OSSTMM debe cumplir con las reglas establecidas en las diferentes Leyes tanto Internacionales, Federales, Locales, Industriales y Políticas establecidas en la organización.

Cada una de las acciones debe prever no violar alguna ley, reglamento o política y cada una de las actividades deben ser coordinadas con la organización que requiere la implementación de este tipo de pruebas a su seguridad.

Este manual también contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL entre otras. Lo que hace de este manual uno de los más completos en cuanto a la aplicación de pruebas a la seguridad de la información en las instituciones.

1. **Propósito.**

   Su principal propósito es proveer de una metodología científica al examinar la seguridad en una organización.

Un segundo propósito es proveer guías para el auditor destinadas a la certificación de la organización.

2. Ámbito

El documento provee una serie de descripciones específicas para el desarrollo de un test de seguridad operacional sobre todos los canales incluyendo aspectos físicos, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción derivada de una métrica real.

3. Resultado Final

- Hora y fecha del Test.
- Duración del Test.
- Tipo de Test.
- Ámbito del Test.
- Índice del Test (enumeración por objetivos).
- Canales testeados o verificados.
- Vectores.
- Verificaciones y cálculo de métricas de los niveles de protección operacional, controles perdidos y limitaciones de la seguridad.
- Conocimiento de que pruebas pueden ser completadas, no completadas o que pueden ser completadas solo parcialmente.
- Cualquier publicación del Test y la responsabilidad de los resultados.
- Los márgenes de error.
- Cualquier proceso que influya en la limitación del Test.
- Cualquier conocimiento de anomalías.

2.3.2 Tipo de Test

Las pruebas de seguridad pueden abarcar todas las formas y tipos como la intrusión hasta la auditoría guiada.

En el OSSTMM contempla 6 tipos de Test.

1. **Blindado:** El auditor establece el objetivo sin el conocimiento de su defensa, activos o canales. El objetivo es preparado para la auditoría conociendo todos los detalles de la misma. En este tipo es lo que se conoce también como “Hacking Ético”.

2. **Doble Blindaje o “Double Blind”:** El objetivo no es notificado con anticipación de los alcances de la auditoría, canales de prueba o prueba de vectores. Este también se conoce como Auditoría de Caja Negra o Pruebas de Penetración.

3. **De Caja Gris:** El Auditor establece el objetivo con un conocimiento limitado de su defensa, activos y todos los canales conocidos. El objetivo es preparado para la auditoría conociendo el avance y detalles de la misma.

4. **Doble Caja Gris:** El auditor establece el objetivo con conocimiento limitado de la defensa, activos y sus canales. El objetivo es notificado del ámbito y tiempo de cada marco de la auditoría pero no de los canales puestos a prueba ni de los vectores.

5. **Tándem o Secuencial *(Tandem)*:** El auditor y el objetivo están preparados para la auditoría y ambos conocen los avances y detalles de la auditoría. Se establece una serie de pruebas de protección *(Tandem test)* y controles del objetivo. Es una prueba minuciosa de acuerdo al visión del auditor del total del análisis. Este es un proceso transparente por lo que se le llama de Caja de

Cristal en el cual tanto el auditor como el objetivo trabajan en las pruebas.

6. **Inverso:** El auditor participa con el objetivo de manera completa en el proceso de la seguridad operacional. Pero el objetivo no conoce el ¿Qué?, ¿Cómo? Y ¿Cuándo? el auditor realizará las pruebas. La meta es desconocida en este tipo de pruebas. La amplitud y profundidad depende de la calidad de la información provista al auditor. Esto permite por lo regular lo que se llama un Ejercicio de Equipo Rojo *(Read Team Exercise)*.

2.3.3 Ámbito o competencia

El ámbito debe abarcar toda la seguridad operativa y comprometerse en las diferentes áreas o canales como lo describe el manual: Seguridad en las comunicaciones, Seguridad Física y Seguridad del Espectro electromagnético, como se muestra en la Tabla 2.3.3-1.

Canal	Sección	Descripción
Seguridad Física	Humano	Todo el elemento humano comprometido en la organización
	Físico	Todo lo referente a instalaciones y cualquier objeto tangible en la organización.
Seguridad de las Comunicaciones.	Redes de datos	Incluye todos los sistemas electrónicos y redes de datos que interactúan en la organización.
	Telecomunicaciones	Son todas las comunicaciones digitales o analógicas empleadas para la comunicación entre redes.
Seguridad del espectro electromagnético	Comunicaciones Inalámbricas	Se incluyen todas las señales electromagnéticas empleadas tanto en las comunicaciones como cualquier otra emanación del espectro.

Tabla 2.3.3-1 Ámbito o competencia de la seguridad.

2.3.4 Módulos

El flujo del manual OSSTMM comienza con situación del objetivo. La situación está dada por la cultura, reglas, normas, regulaciones, legislación y políticas definidas en el objetivo. Y al final se obtiene una comparación de todas las alarmas, alertas, reportes o registros de accesos.

Esta metodología propone un modelo jerárquico de “CANALES, MÓDULOS Y TAREAS”

Los Módulos son áreas específicas de cada canal, pudiendo encontrar actividades que se encuentren en la frontera entre dos canales, por ejemplo una red inalámbrica puede ser analizada como una Red de datos y al mismo tiempo en el ámbito del análisis del espectro electromagnético.

En general esta metodología propone dividir el trabajo de la auditoría clasificándolos por canales, módulos y tareas. Los vectores son simplemente las líneas de análisis que apuntan a cada uno de los canales.

2.3.5 PRUEBAS DE SEGURIDAD EN LA RED DE DATOS

Las pruebas de seguridad en la red requieren de la interacción entre la red de datos y el control de acceso del propietario.

Para determinar la calidad de las pruebas se deben tener las siguientes consideraciones:

1. Ignorancia o conocimiento de la legislación involucrada, se deben tomar en cuenta todas las leyes involucradas tanto nacionales, regionales y políticas internas de la organización

2. Derechos de propiedad: Solo se realizarán pruebas en sistemas que estén dentro del ámbito de competencia del analista de la seguridad, evitando invadir o violar la propiedad de los involucrados.

3. Calidad: Se debe procurar la calidad por encima de la cantidad, debiendo evitar realizar una cantidad pruebas que no se realicen a detalle, no por analizar más canales o módulos se descuiden aspectos importantes o críticos de la seguridad.

2.3.6 Esquema general

Antes de describir cada fase y sus actividades se muestra el esquema general para una mayor comprensión del proceso de las pruebas de la seguridad como se muestra en la figura 2.3.6-1.

Fig. 2.3.6-1 Esquema General de las Pruebas de Seguridad.

2.3.7 Fase de reglamentación

Es la fase en la que se establece la dirección de las pruebas, el auditor comienza con la comprensión de la auditoría, los requisitos, el alcance y las limitaciones.

1. Postura de la revisión

El estudio inicial de la postura de las pruebas debe considerar las leyes, ética, políticas, regulaciones industriales y cultura con respecto a la seguridad.

- Política: Revisar y documentar todos los requerimientos de la política de seguridad, integridad y privacidad dentro de su ámbito.

- Legislación y regulación: Revisar y documentar la legislación regional, nacional y cualquier otra regulación industrial que resguarde la seguridad y privacidad de acuerdo a los requerimientos de la organización.

- Cultura: Revisar y documentar la cultura organizacional.

- Era o época: en lo que se refiere a la edad y generación de los sistemas, software y la aplicación de los servicios que se requieren para la operación.

- Partes débiles: Revisar y documentar cualquier sistema, software y aplicación de servicios que puedan causar alguna inestabilidad dentro de la organización.

2. Logística

Esta es la preparación de los canales para el desarrollo de la evaluación necesarios para la prevención de falsos positivos y falsos negativos que nos puedan llevar a resultados inexactos.

- Estructura
- Calidad de la red de datos
- Tiempo

3. Detección activa de verificación

Determinar los controles activos y pasivos de detección de intrusos para filtrar y denegar intentos de las pruebas con anterioridad para reducir los riesgos de corromper los datos de los resultados de las pruebas.

2.3.8 Fase de Definición

En esta fase se define el ámbito de la aplicación. La base de las pruebas de seguridad requiere el conocer el ámbito y el alcance en relación con las interacciones de los objetivos transmitidos con los activos.

1. Visibilidad de la auditoría

Se enumeran los objetivos (blancos de pruebas) en el ámbito que interactúan directa o indirectamente entre los sistemas.

En este punto se observan aspectos como identificación y delimitación del segmento de red, verificar respuestas icmp, es decir, se describen puntos específicos de evaluación, donde se verifica cada servicio, puerto y aplicación de la red.

2. Verificación de accesos

En este punto se deben enumerar todos los puntos de acceso a la red de datos tomando en cuenta el entorno. Se deben revisar 3 aspectos importantes: Los procesos de acceso, Servicios y Autenticación.

3. **Verificación de confianza**

   Se realizan pruebas para comprobar la confianza entre los sistemas buscando un entorno seguro en lo que se refiere al acceso a la información o la propiedad física para lo cual se necesita la identificación y la autenticación.

   Para ellos se realizan pruebas de *"Spoofing, Phising y de abuso de recursos"*

   - Spoofing o Suplantación: Se realizan pruebas de suplantación en la red, probando
   - "Phishing" es una técnica para realizar fraudes electrónicos donde se envía una liga a una página web, donde al acceso o descarga de algún archivo se incluye código malicioso para obtener información o accesos no autorizados. El objetivo es comprobar las direcciones URL de las peticiones o mensajes.

   - Abuso de recursos**:** Probar la profundidad de los accesos a la información y servidores sin necesidad de credenciales o identificación en la organización. Verificar la continuidad de las métricas especialmente el balanceo de cargas para prevenir que usuarios abusen de los recursos.

4. **Verificación de controles**

   Verificar y enumerar la funcionalidad operacional que asegure la disponibilidad de los activos y los servicios. Para este punto se deben realizar las siguientes pruebas:

   - No repudio: Enumerar y probar los sistemas con pruebas de acceso, verificar los registros de accesos, las interacciones con el propietario y buscar cualquier evidencia de repudio o negación del acceso.

- Confidencialidad: Enumerar todas las interacciones de los servicios con su entorno dentro de las comunicaciones verificando líneas seguras por medio del cifrado. Y verificar los métodos de confidencialidad utilizados en las comunicaciones fuera de los límites.

- Privacidad: Enumerar los servicios en el ámbito de las comunicaciones o activos transportados específicos, mediante firmas, identificación personal y todas las interacciones con el fin de proteger la propiedad y los servicios, proporcionando estos, solo a quienes deban ser compartidos o entregados.

- Integridad: Enumerar las deficiencias y poner a prueba la integridad de los activos y servicios, comprobando que estos no puedan ser modificados o alterados sin autorización y conocimiento del propietario.

2.3.9 Fase de Información

En esta fase el auditor va descubriendo información, aquí se expone la mala gestión de la información.

1. Verificación de procesos

En esta etapa se deben realizar pruebas para examinar el mantenimiento de la seguridad funcional en el establecimiento de procesos como se define en la Postura de la Revisión.

- Mantenimiento: Examinar y documentar las líneas de tiempo, oportunidades, accesos y alcance de los procesos para la notificación y respuesta de seguridad de la red y el monitoreo de la seguridad.

- Desinformación: Determinar la medida en que las notificaciones de seguridad y alarmas pueden ampliarse o alterarse con información errónea.

- Proceso diligente conveniente: Mapear y verificar cualquier laguna entre la práctica y los requerimientos determinados en la Postura de Revisión a través de todos os canales.

- Identificación: Documentar y enumerar los objetivos o blancos y los servicios en los que se puede cometer algún abuso.

2. Verificación de Configuración

Se deben revisar todas las configuraciones implementadas en los controles de acceso, aplicaciones y dispositivos.

- Controles de Configuración: Examinar los controles para verificar la configuración de referencia de los Sistemas Operativos, aplicaciones y equipamiento para validar configuraciones seguras. Y examinar las Listas de Control de Acceso (*ACLs*).

- Errores comunes en las Configuraciones: Verificar los servicios disponibles que no son necesarios o redundantes, verificar las configuraciones por default y verificar la administración ya sea local o remota.

- Mapeo Sensible: Mapear las limitaciones de seguridad descubriendo la áreas sensibles, realizar el análisis de procedimientos actuales, manejo de información confidencial y sensible y la relación con las políticas de seguridad.

- Sensibilidad al *"Hijacking"*: El "*hijacking"* es un término empleado en aspectos de seguridad informática que se aplica para el robo, o por decirlo de otra forma, secuestro de información, sesión o algún activo. Para este punto se debe descubrir y examinar la medida en que personas no oficiales que puedan proporcionar información errónea con el fin de obtener información o acceso no autorizado.

3. Validación de Propiedad

Probar y examinar información y datos disponibles que sirvan para obtener una autenticación ilegal.

- Compartir Recursos: Verificar el grado en que un recurso o licencia individual, privada, que no se reproduce, no libre o no abierta es compartida ya sea intencionalmente o mediante el intercambio de procesos, programas, bibliotecas o involuntariamente mediante una mala gestión de licencias o recursos.

- Mercado Negro: Verificar el grado en que un recurso o licencia se promueve o comercializa ilegalmente por personal o por la organización.

- Canales de venta: Comprobar si alguien fuera del ámbito de la organización vende activos propiedad de la organización.

4. Revisión de Segregación

Realizar pruebas para verificar la separación de la información personal privada y la de la organización.

Se requiere ubicar las localidades más importantes de información privada.

5. **Verificación de Exposición**

   Se deben realizar pruebas para descubrir información que proporcione acceso un área y que permita múltiples accesos a otras áreas.

6. **Exploración de la Inteligencia Competitiva**

   Realizar pruebas de barrido de información que pueda ser analizada como inteligencia de negocio. Esto puede ser con fines de espionaje industrial.

   No se limita a las relaciones comerciales, también incluye empleados, socios, distribuidores, contactos, finanzas, estrategias y planes.

2.3.10 Fase Interactiva de pruebas de controles

Estas pruebas se centran en la penetración y perturbación. Es por lo regular la fase final de las pruebas de la seguridad y esta fase no puede ser realizada hasta que las otras fases se hayan terminado.

Es probable que sea necesario revisar y repetir pruebas que no arrojaron resultados para confirmar los datos.

1. **Verificación de cuarentena**

   Probar y verificar las áreas de contención de elementos agresivos y hostiles para la organización. Se deben tomar en cuenta dos puntos:

   - Identificación y contención de procesos: Identificar y examinar los métodos de cuarentena para contener elementos hostiles como agentes de ventas, caza recompensas, personal de paso por la organización, personal de la competencia y cualquier elemento que

pueda obtener algún beneficio de la información. Esto aplica a procesos automatizados en la red de datos.

- Niveles de contención: Verificar el estado de contención y el tiempo de contención.

2. Auditaría de Privilegios

Se deben realizar pruebas a las credenciales de usuarios y los permisos con los que cuentan.

Para ello se debe examinar la identificación, autorización y el escalamiento.

3. Validación de Sobrevivencia

Determinar y medir la resistencia de los objetivos auditados a los cambios excesivos u hostiles a los que puedan estar propensos.

La denegación de servicio es una situación donde una circunstancia, intencional o accidentalmente, impide que el sistema funcione correctamente, y es común que un sistema funcione incorrectamente en ciertas condiciones como el aumento de carga o el cambio de algunos parámetros.

Para ello se debe verificar tres aspectos:

- Resistencia: Detectar los puntos individuales de fallo, verificar el impacto y las consecuencias en la operación.

- Continuidad: Enumerar y probar los tiempos de respuesta para que se restaure el sistema.

- Seguridad: Mapear y documentar los procesos de apagado de los sistemas en caso de emergencia.

4. **Revisión de Alertas y Registros**

   Realizar un análisis de las deficiencias entre las actividades realizadas con las pruebas y la verdadera profundidad de las actividades registradas.

   - Alarmas: Verificar y enumerar el uso de un localizador de eventos, registros, avisos de peligro o mensajes de accesos donde se conozca o sospeche de ataques, ataque por ingeniería social, intentos o cualquier actividad fraudulenta.

   - Almacenamiento y recuperación: Se debe documentar y verificar los accesos no privilegiados a las alarmas, registros y notificaciones a los sitios de almacenamiento.

CAPÍTULO 3

DESARROLLO DE UN ESQUEMA GENERAL DE UN LABORATORIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

3.1 INTRODUCCIÓN

En este capítulo se propone de forma esquemática la organización y el funcionamiento del Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en Redes de Cómputo (LAVPP) dentro de un ámbito institucional, donde se considera la colaboración con un Área de Gestión y Normatividad (AGN) y un Centro de Operaciones de Seguridad *(SOC por sus siglas en inglés)*.

El laboratorio propuesto, implementa una organización modular con el fin de contar con equipos móviles que cuenten con las herramientas necesarias para realizar análisis y pruebas de seguridad en redes externas.

Asimismo se prevé que el LAVPP pueda operar de manera independiente y autónoma aceptando las solicitudes directas del área usuaria y entregando los reportes a la misma.

3.2 ESQUEMA GENERAL

Se propone el diseño de un LAVPP bajo un esquema general de interacción con un AGN y un SOC.

El AGN tiene la función de realizar los requerimientos necesarios de análisis y pruebas de seguridad al LAVPP, al mismo tiempo de normar y supervisar las actividades que el laboratorio realice.

El SOC recibe la información del AGN para realizar las correcciones que sean necesarias.

Estos procesos de describen en el esquema general que se muestra en la figura 3.2-1.

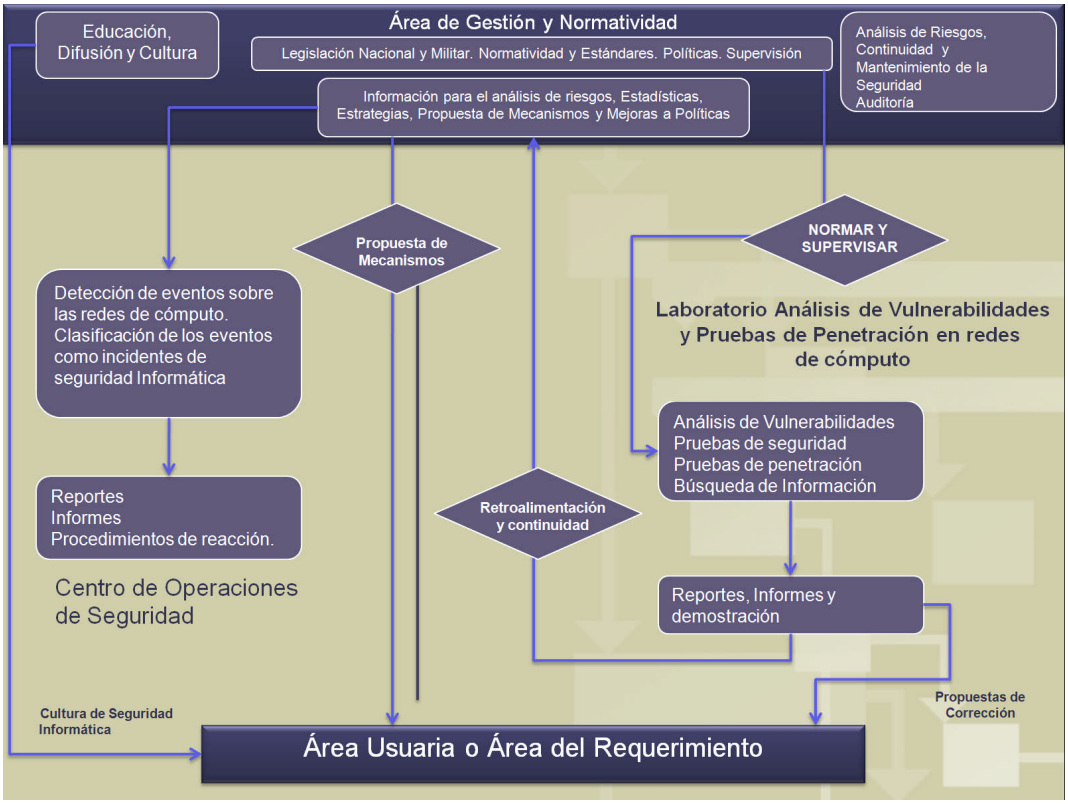

Fig. 3.2-1 Esquema General del Laboratorio de Análisis de Vulnerabilidades y Pruebas de Penetración en redes de cómputo.

Los reportes se pueden entregar al área usuaria en caso de ser necesario como se describe a detalle en el punto 3.4.1 inciso 3.

En caso de no contar con un AGN y un SOC, el laboratorio podrá operar de manera independiente, atendiendo solicitudes o requerimientos del área usuaria y entregando los reportes a la misma, proponiéndole los mecanismos necesarios para las correcciones de las fallas detectadas.

3.3 DESCRIPCIÓN DEL PROCESO GENERAL

El proceso general consta de 3 partes principales que son los requerimientos, el proceso de análisis y los reportes y recomendaciones.

En la figura 3.3-1 se muestra el diagrama general de estos procesos mencionados:

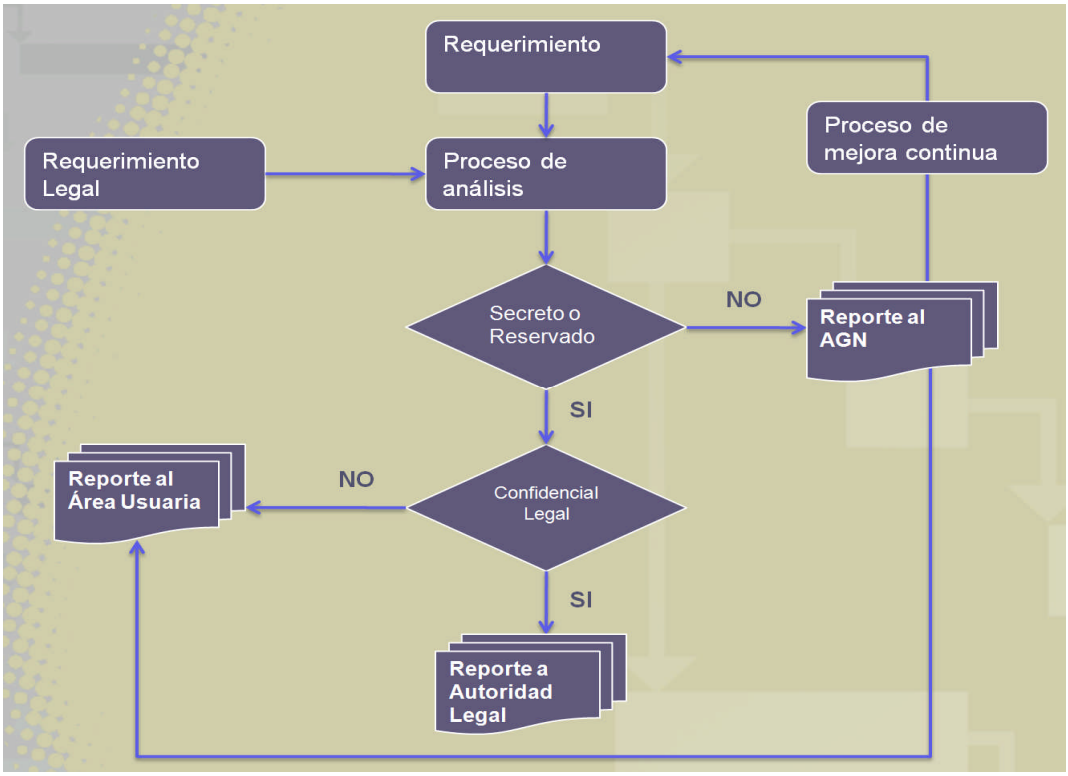

Fig. 3.3-1 Diagrama del proceso general.

Se prevé dos tipos de requerimientos: Requerimiento por parte del AGN o del área usuaria y Requerimiento Legal solicitado u ordenado por una autoridad competente.

Si la información es de carácter Secreto o reservado los reportes serán entregados a la Autoridad Competente o el Área Usuaria dependiendo de la situación.

En caso contrario, los reportes serán entregados al AGN para su aplicación y seguimiento.

3.4 PROCESOS Y FUNCIONES

En este punto se describe el funcionamiento general del LAVPP en relación con su entorno, como ya se explico anteriormente, este puede trabajar como parte de un Sistema de Gestión de la Seguridad o de manera

independiente. A continuación se muestra en la figura 3.3-1 el esquema general de procesos del LAVPP.

Fig. 3.3-1 Esquema general de procesos del LAVPP

En este capítulo se abordan solo los procesos generales y el funcionamiento de acuerdo a la estradas y salidas del laboratorio propuesto. Los procesos a detalle se describen en el capítulo 4.

3.4.1 Funciones

1. Realizar análisis de vulnerabilidades en las redes de cómputo que se requieran, ya sea por solicitud, requerimiento legal o en reacción a un evento relacionado con probables fallas en la seguridad.

2. Realizar pruebas de penetración en redes de cómputo bajo las mismas condiciones que el inciso 1.

3. Entregar los reportes a las áreas interesadas y cuando sea necesario por aspectos de confidencialidad a las áreas o autoridades competentes.

4. Entregar un informe ejecutivo y técnico al área de Gestión y Normatividad para que de seguimiento y realice el proceso de mejora continua.

5. Realizar demostraciones de penetración de sistemas en redes de cómputo con fines de educación, difusión y cultura de seguridad informática.

3.4.2 Entorno

El laboratorio propuesto puede funcionar de dos formas:

1. En una red de datos aislada completamente, realizando pruebas controlados con el fin de ejecutar diferentes tipos de ataques, los que pueden incluir código malicioso y evitar daños en las áreas de producción.

2. Con los equipos móviles colocarlos en los puntos estratégicos en una red de datos con el fin de realizar diferentes análisis y pruebas de la seguridad, previendo cualquier fallo o denegación de servicio por las aplicaciones que se ejecuten.

3.4.3 Entradas (Solicitudes y requerimientos)

Las necesidades de análisis y pruebas de la seguridad pueden surgir en base a 3 situaciones:

1. Por solicitud expresa del AGN.

2. Por solicitud expresa del Área Usuaria

3. Por requerimiento legal

4. En respuesta a eventos o incidentes

3.4.4 Salidas (Informes entregables al AGN)

La información que se entrega al AGN, tiene cuatro propósitos:

1. Informar al área usuaria de las deficiencias de seguridad en tecnologías de la información que se detectaron durante las pruebas y el análisis.

2. Proporcionar información al SOC, para que proponga los mecanismos necesarios y realice las implementaciones y correcciones que se requieran para mitigar las vulnerabilidades y los riesgos.

3. Dar seguimiento de los resultados obtenidos, con el fin de supervisar que las fallas detectadas sean subsanadas.

4. Correlacionar la información generada con la de otras áreas con el fin de proponer las estrategias que ayuden a mejorar la operatividad, funcionalidad y seguridad de la Organización y proporcionando información gerencial para la toma de decisiones.

3.4.5 Informes entregables al Área Usuaria

Los informes solo se entregarán al área usuaria en las siguientes condiciones:

1. Cuando por seguridad, ninguna área de la organización deba conocer información relacionada y generada del análisis y pruebas realizadas. Con el fin de mantener el secreto de la información, los reportes se entregan directamente al área usuaria.

2. Cuando el área usuaria cuente con el personal, equipo y presupuesto para implementar los mecanismos de seguridad propuestos y con el fin de disminuir los trámites y tiempos de implementación. Este aspecto debe considerarse por cuestiones de urgencia de implementación o por orden expresa de la alta gerencia o Dirección General de la Organización.

3.4.6 Ámbito o Competencia

1. El LAVPP se propone para su aplicación en Instituciones Federales, el cual puede ser incorporado a un Sistema Integral de Seguridad o funcionar de manera independiente.

2. Su trabajo se limita a realizar análisis y pruebas de la seguridad en Instituciones gubernamentales por requerimientos de alguna autoridad competente.

3. Se realizarán informes preliminares y detallados de los resultados obtenidos durante las pruebas y análisis que se realicen.

4. Se realizarán la pruebas y análisis correspondientes en base a el Manual de la Metodología Abierta de Testeo de la Seguridad OSSTMM del ISECOM y con el apego a las leyes vigentes en México.

5. Se emplearán herramientas automatizadas tanto comerciales como de software libre para el desarrollo de las pruebas, las cuales se describen en el capítulo cuatro.

3.4.7 Requerimientos

Se propone el equipamiento del LAVPP con software y equipo redundante con el fin de contar con equipos móviles con los que se puedan hacer análisis y pruebas de la seguridad en otras instalaciones sin detrimento de la operatividad del mismo.

1. **Software**

   2 Sistemas de Intrusión Informática.
   2 Software de análisis de vulnerabilidades en redes.
   2 Software de análisis de vulnerabilidades en Web.
   2 Software de pruebas de penetración en redes de cómputo.

2. **Hardware**

   8 Equipos de cómputo
   1 Servidor
   3 Switch 24 puertos 10/100/100

2 Ruteadores

1 Ruteador Inalámbrico

3. **Personal**

   8 Personas con conocimientos técnicos en informática con el fin de contar con dos personas y mantener la continuidad y permanencia de las actividades del laboratorio.

3.4.8 Esquema de la Propuesta de estructura física con hardware, software y para la implementación del LAVPP.

Se propone una estructura física conformada por equipos de cómputo móviles (Laptop) y herramientas de software para el análisis de seguridad como se muestra en la figura 3.4.8-1.

Las pruebas pueden realizarse en un ambiente controlado por medio de la emulación de equipos, aplicaciones y servicios.

Los equipos y software deben ser redundantes, con el propósito de estar en condiciones de mover el equipo que sea necesario para realizar análisis en redes externas sin detrimento de la operatividad del LAVPP.

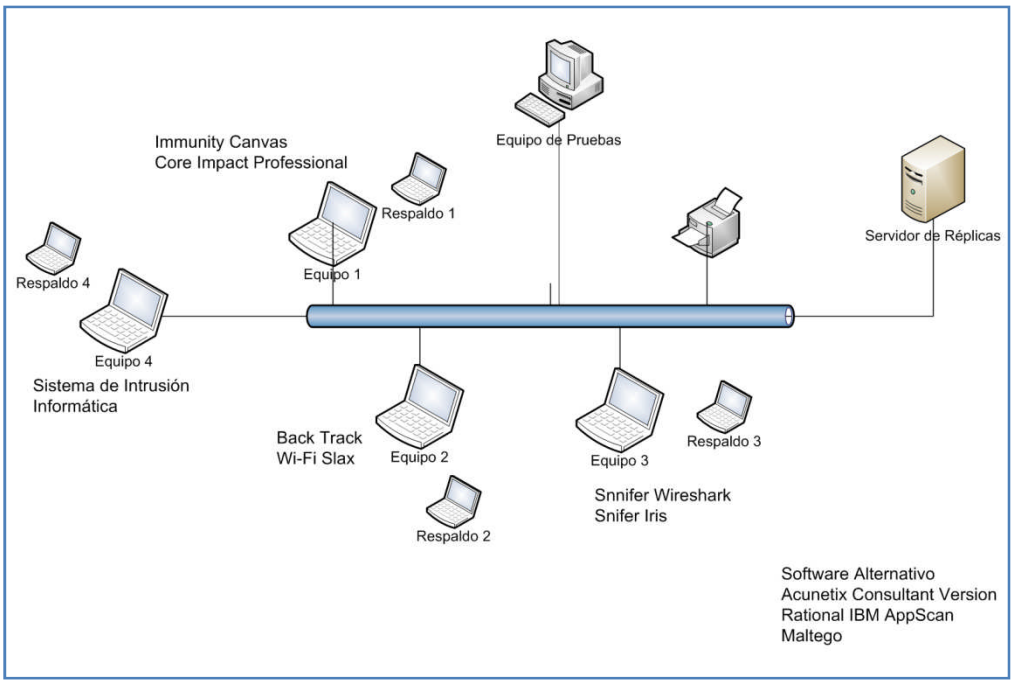

Fig.3.4.8-1 Esquema de la propuesta de estructura física para el LAVPP

CAPÍTULO 4
MARCO LEGAL

4.1 INTRODUCCIÓN AL MARCO LEGAL

El conocimiento y delimitación del marco legal relacionado a las pruebas de la seguridad protegen al analista de incurrir en un delito o faltas administrativas que puedan perjudicarlo e interrumpir los procesos de las pruebas.

En la presente tesina se mencionan y citan textualmente las leyes de carácter federal de interés en proceso de análisis, pruebas y manejo de la información. Las leyes locales pueden variar de acuerdo con el Estado donde se encuentre, por lo que no se describen en el texto.

4.2 CONSIDERACIONES LEGALES.

Es necesario que antes de realizar algún análisis o pruebas a la seguridad en una organización, se deben prever y contemplar todas las leyes, reglamentos y políticas relacionadas con el manejo de la información, la propiedad privada e intelectual y los reglamentos y políticas de la organización como se describe a detalle a continuación:

1. Solicitud y autorización por escrito de la organización en la que se realicen las pruebas a la seguridad.

2. En caso de ser necesario, firmar contrato de confidencialidad por los resultados que puedan obtenerse y que comprometan la seguridad de la organización.

3. Conocimiento y coordinación con la organización de cada una de las pruebas, así como de los alcances y riesgos que puedan existir.

4. Diferenciar y separar los recursos e información que son propiedad de la organización y los que son propiedad privada.

5. Informar a quien corresponda de la organización de los resultados que se vayan obteniendo durante el transcurso de las pruebas.

6. Contemplar las leyes vigentes de carácter federal, local y en los casos que se requiera las leyes internacionales.

7. Conocer las reglamentaciones industriales y políticas organizacionales respetando cada una de ellas.

4.3 Código Penal Federal

El Código Penal Federal contempla algunos de los delitos informáticos en los que se pueda incurrir con un mal análisis.

1. Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

   Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

2. **Artículo 211 bis 2**. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

   Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

3. **Artículo 211 bis 3**. Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

   Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

4. **Artículo 211 bis 4**. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

   Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

5. **Artículo 211 bis 5**. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

   Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de

tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

6. **Artículo 211 bis 6.** Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este código.

7. **Artículo 211 bis 7.** Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

4.4 Ley Federal de Derechos de Autor

Dicha ley contempla en su Capítulo IV (De los programas de computación y las bases de datos) lo siguiente:

1. **Artículo 102.** Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

2. **Artículo 103.** Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

3. **Artículo 106.** El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, concluido el alquiler, y

IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

4. **Artículo 109.** El acceso a información de carácter privado relativa a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

5. **Artículo 112.** Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de

telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

6. **Artículo 113.** Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

7. **Artículo 114.** La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

CAPÍTULO 5

PROPUESTA DE IMPLEMENTACIÓN DEL LABORATORIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN.

5.1 PROCESOS DE LAS PRUEBAS DE SEGURIDAD.

En este punto se describen las propuestas de los procesos que se deben llevar a cabo para el desarrollo de las actividades del LAVPP.

Es importante mencionar que en todo análisis y pruebas que se realicen, se deben tomar en cuenta todas las fases y procesos mencionados en el capítulo3.

Al mismo tiempo se realizan adaptaciones para la comprensión de los procesos sin alterar el objetivo o la metodología empleada como base.

5.1.1 Requerimientos y Solicitudes

Los requerimientos y solicitudes pueden ser recibidos de tres formas o de tres posibles áreas.

1. Requerimiento del AGN

2. Requerimiento del Área Usuaria

3. Requerimiento Legal

Estos requerimientos o solicitudes se deberán hacer por escrito e indicar los antecedentes, motivos y marco legal sobre el que se deberán realizar.

5.1.2 Coordinación con área usuaria.

Es necesario establecer plena coordinación para la ejecución de los trabajos necesarios, por lo siguientes motivos:

1. Evitar violar alguna ley federal, local, institucional.

2. Evitar provocar fallos en el funcionamiento de los sistemas que se encuentren en producción.

3. Mostrar absoluta transparencia en los procesos, con el fin de mostrar y comprobar que los fallos encontrados no son provocados por el personal analista o auditor.

4. Definir e tipo de Test, de acuerdo al punto 2.3.2.

5. Definir el ámbito de competencia de las pruebas, las cuales se describen en el capítulo 2.3.3.

5.1.3 Situación actual y Definición de Estrategias.

En este punto de busca establecer el mejor camino para la obtención de resultados verídicos, confiables oportunos. Para ello se definen diferentes aspectos como a continuación se indica:

1. Descripción y enumeración de procesos.

2. Delimitación del o los segmentos de red y definir las periferia en cada uno de los casos.

3. Nombres y ubicación de servidores.

4. Cantidad de terminales.

5. Balanceo de cargas.

6. Respuestas ICMP.

7. Respuestas TCP y UDP

8. Trazado de rutas por medio de paquetes ICMP, TCP y UDP.

9. Enumerar los protocolos y servicios.

10. Examinar encabezados correo electrónico.

11. Búsqueda de registros de intrusiones previas.

12. Examinar objetivos de aplicaciones basadas en web.

13. Verificar respuestas y reacciones a paquetes SYN, SYN ACK, ACK, RST Y FIN.

14. Verificar respuestas y reacciones a paquetes TCP con cambio en las banderas.

15. Verificar respuestas en cuanto al TTL.

5.1.4 Verificación de accesos

En este punto se deben enumerar y probar todos los puntos de acceso a la red y en la red.

1. Verificación y pruebas de conexiones UDP.

2. Verificación y pruebas de conexiones VPN.

3. Descubrimiento de puertos TCP

4. Búsqueda de interacciones de servicios en el que procesos débiles comprometan accesos.

5. Revisar interacciones de puertos con servicios o “demonios”, así como aplicaciones que hagan uso de servicios y protocolos.

6. Verificar servicios de Voz sobre IP (VoIP)

7. Enumerar los accesos que requieren autenticación y documentar los privilegios con los que cuentan.

8. Verificar los métodos de identificación y autorización requeridos.

9. Verificar el método de autentificación.

10. Verificar contraseñas y su fortaleza.

5.1.5 Verificación de confianza

Para este punto se realizan tres pruebas principalmente, lo que se conoce como “Spoofing” o suplantación, el “Phishing” lo que puede traducirse para su comprensión en el envío de anzuelos y el uso y abuso de recursos.

1. Spoofing por obtención y pruebas de direcciones IP válidas.

2. Spoofing por inundación ARP, provocando alteración de las tablas ARP de las terminales con lo que se intercepta las comunicaciones.

3. Phishing por medio de envío de direcciones URL, que son anzuelos para que usuarios con exceso de confianza realicen accesos a las direcciones recibidas y sean víctimas de múltiples ataques.

4. Verificar la legitimidad de las direcciones URL a las que se tiene acceso por los usuarios de la red.

5. Probar accesos por medio de cuentas o credenciales y cualquier otra información disponible.

5.1.6 Verificación de controles

Probar, enumerar y verificar la funcionalidad operativa de los activos y servicios.

1. Realizar pruebas de uso inadecuado de demonios, servicios y sistemas con el fin de obtener accesos o información para diferentes fines.

2. Verificar todos los métodos de interacción con el propietario.

3. Enumerar todas las interacciones de los servicios con su entorno, para conocer líneas seguras de transmisión, transporte de información por medios electrónicos, dispositivos de almacenamientos, documentación y cualquier elemento que contenga datos de la organización.

4. Verificar todos los procesos empleados para mantener la confidencialidad.

5. Verificar los límites de la seguridad en las comunicaciones.

6. Verificar los procesos dedicados a la integridad de los activos como funciones hash, marcas de agua, cifrado, marcas o identificadores en equipos, etc.

5.1.7 Verificación de procesos

1. Examinar y documentar la oportunidad, conveniencia, el acceso y el alcance de los procesos de notificación y respuesta de seguridad en lo que respecta a la red de vigilancia y monitoreo.

2. Determinar la medida en que las notificaciones, registros y alarmas pueden ser alteradas o modificadas con información erróneas.

3. Mapear y verificar las lagunas o faltantes entre la práctica y los requerimientos determinados en la Postura de la Revisión a través de todos los canales.

4. Documentar y enumerar los objetivos y los servicios que estén protegidos.

5. Enumerar y examinar las pólizas de seguros sobre los activos.

5.1.8 Verificación de configuración

1. Examinar los controles para verificar las configuraciones de los Sistemas Operativos, aplicaciones y equipos en aspectos de seguridad y mejores prácticas.

2. Examinar las listas de control de acceso (ACL) que cumplan con el propósito de la organización.

3. Buscar servicios redundantes innecesarios.

4. Buscar configuraciones por default.

5. Verificar que la administración se realice a nivel local, en caso de realizarse de manera remota, realizar todas las pruebas al proceso de administración completo.

6. Revisar las configuraciones de Sistemas Operativos, aplicaciones y equipos.

5.1.9 Validación de propiedad

1. Revisar el proceso de gestión de licencias y recursos.

2. Verificar que las licencias y recursos no se comercialicen en el interior o exterior de la Organización.

5.1.10 Revisión de segregación

1. Mapear los tipos de información y detectar información de propiedad privada, propiedad de la organización y pública.

2. Mapear los repositorios de información.

3. Mapear la propiedad de la información y verificar si son acordes a las políticas y regulación de la organización.

4. Mapear las interacciones, es decir, identificar quienes tienen acceso y hacen uso de la información.

5.1.11 Verificación de exposición

Enumerar información relativa a la organización y todo lo que de información de las políticas de la organización:

1. Organigramas
2. Diagramas
3. Nombramientos y puestos.
4. Descripción de puestos de trabajo.
5. Números telefónicos de la organización y del personal.
6. Tarjetas de visita.
7. Documentos compartidos.
8. Currículum Vitae
9. Afiliaciones de la Organización.
10. Direcciones de correo electrónico
11. Contraseñas.

5.1.12 Inteligencia competitiva

Se debe recopilar toda la información de Inteligencia del negocio.

1. Enumerar puntos de acceso

2. Información del almacenamiento de la información (que se almacena, como se almacena y cada cuando se almacena).

3. Perfil de la organización: Giro de la organización, perfil de los empleados, escalas salariales, tecnologías, tipos de datos, carteras de clientes.

4. Socios, clientes, proveedores, distribuidores, inversionistas, relaciones comerciales, producción, desarrollo, productos, planes y bienes.

5. Enumerar personal estratégico de la organización.

6. Tipos de divulgación de la organización.

7. Manuales y políticas públicos.

8. Análisis de procesos desde un plano externo.

5.1.13 Verificación de cuarentena

Verificar la contención de contactos hostiles.

1. Identificar y examinar los métodos de contención.

2. Nivel de contención: estado, tiempo y acciones.

5.1.14 Auditoría de privilegios

1. Examinar y documentar los procesos de autorización.

2. Identificar los diferentes métodos de acceso.

3. Enumerar los permisos y privilegios.

4. Verificar los medios fraudulentos para obtener la autorización.

5. Probar y enumerar las cuentas y contraseñas por defecto de la configuración.

6. Pruebas acceso por fuerza bruta u obtención de contraseñas.

7. Pruebas de escalamiento de privilegios.

5.1.15 Verificación de sobrevivencia de Sistemas

1. Verificar puntos de fallos causados por cambios, actualizaciones y modernización de la infraestructura y tecnología.

2. Verificar los privilegios inducidos por los fallos mencionados en el punto anterior.

3. Enumerar insuficiencias en relación con accesos y retrasos.

5.1.16 Revisión de alertas y registros

1. Verificar y enumerar los sistemas de alarmas y registros de eventos.

2. Enumerar, clasificar y documentar los tipos y cantidades de alertas y registros.

3. Verificar el tamaño y calidad de los archivos de que se generen de las alarmas y registros.

5.1.17 Informes y Reportes

Se proponen 3 tipos de reportes:

1. **Reporte técnico.**

   En este tipo de reporte se debe describir a detalle la metodología, procedimientos y resultados usados y obtenidos durante las pruebas realizadas.

   Se debe separar de la misma forma que se realizaron las pruebas, es decir en fases, con el fin de obtener una mayor comprensión y coherencia.

   El reporte debe ir acompañado de una bitácora.

2. **Reporte gerencial.**

   En este reporte se presenta un resumen de los resultados obtenidos.

   Se resaltan los datos de mayor importancia como vulnerabilidades de alto riesgo y potencialmente explotables.

   Debe contener un lenguaje claro con el menor número de tecnicismos.

   Se deben describir las recomendaciones y propuestas de remediación de los fallos.

3. **Reportes preliminares.**

   Este tipo de reporte se emplea en los casos que se cuente con la detección de fallos de carácter urgente que requieran a atención y corrección en el menor tiempo posible.

CONCLUSIONES

1. El análisis de vulnerabilidades en redes de cómputo previene de fallos a la seguridad en el manejo de la información por medios informáticos. Se disminuyen los riesgos de robo, pérdida o alteración de la información, así como de otros activos de una organización.

2. Las pruebas de penetración sirven para demostrar el personal de usuarios y directivos las acciones y consecuencias perjudiciales en la operatividad, administración y logística de la organización cuando se presenta un evento de seguridad negativo, ya sea por mal uso de los sistemas, ataques desde el interior o exterior de la red, fallas en el suministro de energía y cualquier otra situación no prevista.

3. Proporcionar información de los resultados a un Área de Gestión y Normatividad sirve para dar continuidad y seguimiento a la corrección de las fallas detectadas, prevenir incidentes y accidentes, contar con información estratégica para la toma de decisiones y fomentar la educación y cultura de la seguridad informática en una Organización.

REFERENCIAS BIBLIOGRÁFICAS

[88] Autor (apellido, nombre), titulo, editorial, edición, país, año, numero de paginas.

[51] Comunicaciones y redes de computadoras 7ª edición, Editorial pp 519

[88] Richardson Robert, **"The latest results from the longest-running project of its kind"**, CSI Computer Crime & Security Survey, 2008

[51] **"Manual de la Metodología Abierta de Testeo de la Seguridad 3.0"**, (OSSTMM), ISECOM, 2009

[88] **"Penetration Testing Framework",** Information Systems Security Assessment Framework (ISSAF), Draft 0.2 1B, mayo 2006

[88] Scarfone Karen, Souppaya Murugiah, Cody Amanda, Orebaugh Angela, **"Technical Guide to Information Security Testing and Assessment"**, National Institute of Standards and Tchnology (NIST) SP800-115, Septiembre 2008

[88] Bowen Pauline, Hash Joan, Wilson Mark, **"Information Security Handbook: A Guide for Managers"**, National Institute of Standards and Tchnology (NIST) SP800-100, Octubre 2006

[88] Ross Ron, Katzke Stu, Johnson Arnold, Swanson Marinne, Stoneburner Gary, Managing Risk from Information System, National Institute of Standards and Tchnology (NIST) SP800-39, Abril 2008

[ ] ISO 27001

[ ] ISO 27002

[99] Parziale Lydia, Britt David T., Davis Chuck, TCP/IP Tutorial and Technical Overview, Redbooks IBM, Diciembre 2006

[55] J. Postel, J Reynolds, Telnet Protocol Specification, RFC854, Mayo 1983

[88] Internet Protocol Darpa Internet Program, rfc791, Defense Advanced Research Project Agency, Arlintong Virginia Septiembre 1981

[88] Plumer David C., Noviembre, Ethernet Address Resolution Protocol. 1982, rfc 826

[88] Transmission Control Protocol, darpa internet program, rfc 793, sep 1981, Defense Advanced Research Projects Agency Information Processing Techniques Office

[88] J. Postel, rfc 768- User Datagram Protocol, agosto 1980

[99] J. Postel, J. Reynolds, rfc 959 File Transfer Protocol, Octubre 1985

[88] J. Mogul, RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1, Network Working Group