UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO Y DESARROLLO DE HERRAMIENTAS PARA EL ESTUDIO DE LA SEGURIDAD INFORMÁTICA

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

PEDRO BECERRIL FAJARDO

DIRECTORA DE TESIS:

M. C. MA. JAQUELINA LÓPEZ BARRIENTOS

CIUDAD UNIVERSITARIA, 2007.

Agradecimientos

A mis padres, Abel Becerril Gil y Gloria Fajardo Zuñiga, quienes me apoyaron y auxiliaron durante todo este tiempo, a mis hermanos, Abel Becerril Fajardo y Cynthia Becerril Fajardo, y a mi tía Glafira Fajardo Zuñiga, quienes colaboraron de manera indirecta en la realización y conclusión del presente trabajo, a mi asesora M. C. MA Jaquelina López Barrientos quien me brindó su asesoría, tiempo, conocimientos y consejo para la elaboración de este proyecto, al "Laboratorio de Investigación y Desarrollo de Software Libre" (LIDSOL) por brindarme las facilidades y tiempo para adentrarme al mundo del software libre, particularmente a Alan Edgar García Flores y Carlos Franco Díaz, quienes siempre me brindaron su apoyo y ayuda a lo largo de este trabajo, a Gustavo Gómez Macías e Isset Guerrero Galache quienes de una u otra forma me ayudaron a que el proyecto siguiera adelante, a Luis Gerardo Tejero Gómez, cuya aportación a la presente investigación resultó imprescindible, a José Guadalupe Serrato Cervantes y Uriel Canto Arce, quienes aportaron ideas, recomendaciones e hicieron diversas correcciones, a todas las personas que participaron en la realización de los talleres, particularmente a los integrantes del "Laboratorio de Redes y Seguridad de la Facultad de ingeniería", quienes me brindaron el espacio y tiempo para la realización de las investigaciones, al Lic. Onan Yair Paredes Reyes por su orientación y aportación durante la redacción del presente trabajo, a Julián Garritz Cruz, quien me brindó la oportunidad de ingresar al mundo laboral, y cuya experiencia sirvió para complementar la investigación presente, a la Universidad Nacional Autónoma de México por brindarme la oportunidad de aprender y estudiar dentro de sus aulas, formándome como profesionista, finalmente a todas aquellas personas que he olvidado mencionar pero que de una u otra manera contribuyeron con este proyecto.

Índice

Prefacio

La seguridad en el área de cómputo se ha vuelto de vital importancia en los últimos años. Ya sea para la realización de transferencias bancarias o bien, llevar el control de actas de calificaciones; actualmente es necesario contar con mecanismos que nos permitan proteger nuestra información. Es por ello que surgen diversas medidas para protegerla.

Resulta necesario conocer a fondo el software que se planea utilizar, a fin de evitar filtrado de información, la intrusión de usuarios no autorizados a los datos que se encuentren dentro de la organización, así como evitar pérdidas de información ya sea por virus informáticos o ataques externos; todo esto como resultado de diversos factores, como pueden ser una incorrecta configuración del firewall, o bien, desconocimiento del funcionamiento de los diversos protocolos de red existentes.

Debe quedar en claro que no existen sistemas perfectos, y que siempre estará presente la posibilidad de alguna intrusión o de algún fallo, por lo que es preciso mantener una constante actualización tanto de las políticas de seguridad informática como de los sistemas mismos.

Por consiguiente, es menester que los profesionistas reciban los conocimientos y la preparación indispensables junto con las herramientas necesarias durante su preparación a fin de poder hacer frente a los retos que se presenten durante el ejercicio de su carrera, por lo que se requiere poner en práctica los conceptos teóricos vistos durante el estudio de la carrera.

Por ello, el objetivo del presente trabajo de tesis es diseñar una serie de prácticas que permitan a los estudiantes que cursan la carrera Ingeniería en Computación, aplicar los conocimientos de seguridad informática dentro de un espacio controlado. De la misma manera, se busca proporcionar las herramientas

necesarias que permitan a los estudiantes ampliar sus habilidades y conocimientos en la administración de redes informáticas y mismo modo se conozcan las medidas de seguridad correspondientes.

Así, la realización de este trabajo está enfocada en brindar un aporte a la comunidad universitaria, a fin de que las nuevas generaciones tengan una mejor preparación que los ayude a tener las habilidades necesarias para hacer frente a los retos que en seguridad informática se presenten al ejercer su profesión.

Para lograr los objetivos planteados, en el primer capítulo se dan a conocer el funcionamiento básico de las redes de cómputo, enfocándose al modelo OSI y cómo es que éste describe la manera en que se estructura la interconexión entre computadoras. Por otra parte, también se muestra una serie de conceptos básicos relacionados a la seguridad informática, que más adelante serán necesarios para abordar temas más complejos.

El segundo capítulo aborda el tema referente a las políticas de seguridad, que si bien resulta un tema bastante extenso, se presenta un esbozo que tiene como finalidad dar los principios por los que se debe regir cualquier persona encargada de administrar sistemas informáticos. Aunque en cierto modo los tópicos planteados pueden parecer conceptos bastante teóricos tienen gran aplicación al conjuntarse con la parte técnica dentro de la gestión de los sistemas.

El tercer capítulo muestra de manera general los diversos tipos de amenazas existentes en la actualidad, así como el funcionamiento y el peligro que representa para los usuarios. Así mismo se presentan diversos datos estadísticos que permiten entender la naturaleza de los atacantes de los sistemas y poder establecer mejores estrategias que eviten en la medida de lo posible pérdidas sensibles ocasionadas por este tipo de intrusiones.

El cuarto capítulo es referente a las diversas medidas y herramientas que pueden ser utilizadas para prevenir o combatir ataques e intrusiones. Si bien, existe una gran diversidad de opciones en el mercado para la seguridad informática, resulta necesario conocer la utilidad real que se puede obtener de las diversas herramientas disponibles, adaptándolas de manera conjunta a las necesidades de los usuarios.

La última parte muestra cómo la investigación realizada a lo largo de los capítulos anteriores ha sido condensada en una serie de prácticas de laboratorio, explicando de manera particular cada una de ellas y detallando los diversos criterios que se tuvieron para la elección de software, así como los objetivos que se buscaron cubrir detrás del planteamiento de cada una de ellas.

Finalmente se presentan las conclusiones del trabajo realizado y en las cuales se estipula que se espera que el material proporcionado resulte de utilidad para las futuras generaciones que tengan el interés de ahondar y dedicarse al ramo de la seguridad informática, esperando que las presentes herramientas los ayuden a ampliar su perspectiva dentro del ámbito de la computación.

Capítulo 1

Conceptos Generales

Capítulo 1
Conceptos Generales

El área de seguridad informática abarca una gran diversidad de temas que la hacen ser bastante compleja, ya que no sólo se toman aspectos tecnológicos para su desarrollo, también abarca partes de la conducta humana, los cuales es necesario conocer para entender y poder planificar estrategias que permitan poner en práctica la teoría de la seguridad informática.

Asimismo se requiere partir de las raíces a fin de poder estructurar y entender conceptos más complejos que permitan explotar al máximo los recursos con los que contamos. Dentro del los sistemas informáticos, uno de los grandes pilares en los que se trabaja toda la teoría de redes es el modelo OSI. Por esta razón, es necesario conocer en primer lugar como está estructurado este modelo para poder comprender posteriormente cómo trabajan los protocolos y en consecuencia, los programas encargados de proteger las redes.

Debido a que la tecnología depende completamente de las personas que hacen uso de ésta, se vuelve aún más indispensable conocer qué lineamientos se deben seguir a fin de que el aprovechamiento de los recursos tecnológicos cumplan en la medida de lo posible su función, que es garantizar la integridad y disponibilidad de la información. Es por este motivo que se vuelve necesario conocer los principios de la seguridad informática, ya que con base en éstos es que se planean estrategias y políticas que a corto o largo plazo ayudarán en la operatividad de los sistemas de la información.

Finalmente, a fin de poder aplicar la teoría descrita, es importante conocer la realidad en la que se vive actualmente, por lo que ser conciente de la verdadera dimensión que representa en nuestros días contar con sistemas de protección para los sistemas informáticos nos ayuda a ampliar el panorama general de la importancia que tiene en nuestros días la seguridad informática

1.1.- Panorama Actual

En el mundo contemporáneo, los sistemas de información se han vuelto de vital importancia para toda empresa que desee mantenerse dentro del mercado. Por lo tanto buscar la protección de la información ha ido de la mano con los nuevos avances tecnológicos que se han ido desarrollando en los últimos años. Así entonces, se ha vuelto una necesidad buscar mecanismos que aseguren a las personas que las redes y la información se mantendrán en óptimas condiciones a fin de poder continuar laborando.

La tendencia actual es garantizar que los sistemas de información se mantengan íntegros, ya que de otra manera, esto puede causar graves pérdidas económicas en la compañía o bien, provocar pérdida de prestigio. De la misma manera se exige que haya el menor número de fallas, los usuarios se han vuelto cada vez más exigentes en lo que respecta al funcionamiento de las comunicaciones, por lo que cualquier problema resulta una molestia inadmisible.

Podemos afirmar entonces que la combinación de todas estas tendencias nos exige garantizar la protección a la información, que ésta se encuentre siempre disponible para los usuarios y sea confiable para los intereses de la empresa. Ya que no es posible tener una certeza total de que los sistemas de información siempre estén libres de amenazas, se debe asumir la posición de buscar minimizar al máximo los riesgos y evitar pérdidas por descuidos o negligencias que en su momento pudieron evitarse.

Por lo antes expuesto, es de suma importancia que un administrador de los sistemas de información considere enfocarse en los siguientes puntos:

- Entender, es decir, conocer sobre el entorno que se integra tanto dentro como fuera de la organización. Ser consciente de las amenazas y vulnerabilidades con las que se cuentan y saber cómo minimizar los riesgos originados por dichos factores.

- Actuar, esto es, poder responder de forma inmediata y precisa ante posibles contingencias y ataques a los sistemas de información. De la misma manera es tomar las medidas de precaución necesarias a fin de mantener la información actualizada y sea posible recuperarla en caso de alguna contingencia.

- Controlar, que se refiere a administrar los recursos de los sistemas de comunicación para evitar posibles trastornos que afecten el funcionamiento de la organización y hacer que los usuarios puedan hacer un buen uso de dichos recursos a fin de expandir la funcionalidad de los mismos.

Podemos destacar dentro de los últimos 15 años el crecimiento que ha tenido el uso de Internet, resultando ser uno de los aspectos más complejos el de administrar y controlar desde el punto de vista de las organizaciones, ya que si bien ha resultado ser una herramienta muy potente de comunicación y enlace entre las personas, también ha sido vehículo de diversas amenazas para las organizaciones. Desde virus hasta programas de espionaje circulan actualmente a través de Internet y es por consiguiente necesario establecer las medidas necesarias que garanticen que los usuarios hagan un buen uso de esta herramienta y contribuya en la productividad de las organizaciones.

Del mismo modo que Internet ha visto un crecimiento exponencial por parte del número de usuarios que lo utilizan, los ataques e intrusiones a los sistemas de información también han tenido un crecimiento acelerado. Desafortunadamente este crecimiento también se ha visto reflejado de manera homologa en pérdidas económicas como se puede apreciar en la gráfica de la figura 1.1:

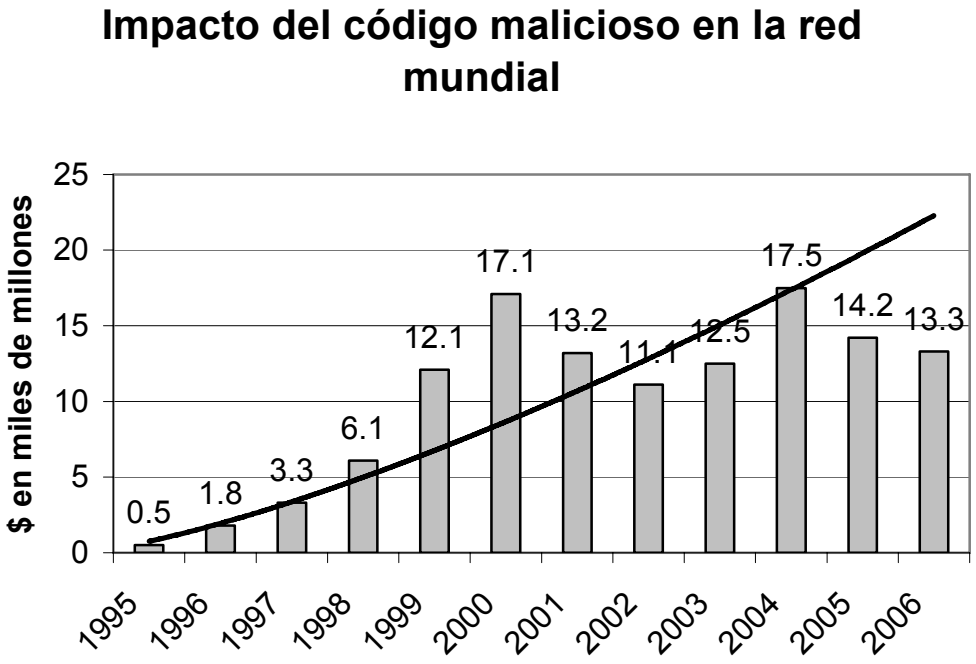


Figura 1.1 – Crecimiento del impacto económico código malicioso a lo largo de los años [1]

Esta situación no puede ser ignorada por las empresas actualmente, ya que las pérdidas ascienden a miles de millones de dólares. Algunos factores que podemos destacar que han incentivado el aumento de problemas dentro del área de la seguridad informática son el incremento en las vulnerabilidades de los sistemas, el arduo trabajo que se requiere para combatir dichas vulnerabilidades y la complejidad cada vez mayor que han tenido los ataques.

Existe una gran diversidad de casos que nos muestran el impacto que en últimas fechas han tenido los ataques a los sistemas de comunicación. Por ejemplo, en el

[1] Fuente: Computer Economics

año 2003, el virus “Código Rojo” infectó 350 000 computadoras en sólo 14 horas. Otro caso es el del virus “MyDoom”, el cual resultó ser el gusano que más rápidamente se propagó vía correo electrónico, siendo que dependía de los usuarios de los equipos para poder activarse.

Amenazas de este tipo resultan muy difíciles de controlar una vez que han sido inicializadas, ya que debido a la velocidad con la que dañan los equipos se vuelve prácticamente imposible poder reaccionar ante este tipo de contingencias. Es ahí donde se requiere hacer énfasis, en la importancia de tener medidas preventivas de seguridad, y es donde se puede entender la importancia de las políticas de seguridad, las cuales resultan ser la parte medular de la protección dentro de las organizaciones.

Se espera que las amenazas sigan creciendo tanto en magnitud y complejidad, lo que significará que será necesario implementar nuevos métodos de prevención y control que permitan a las organizaciones hacer frente a las nuevas amenazas. Un caso reciente de los niveles que han alcanzado las intrusiones en los sistemas de información es dentro del gobierno de los Estados Unidos, quien con el apoyo de la empresa Trend Micro, ha comenzado a investigar cómo es que las computadoras de agencias de gobierno han sido infectadas con programas de minería de datos, spam o han sufrido ataques de denegación de servicios

La gráfica de la figura 1.2 muestra el crecimiento desmesurado que han tenido las amenazas informáticas en los últimos años a nivel mundial:

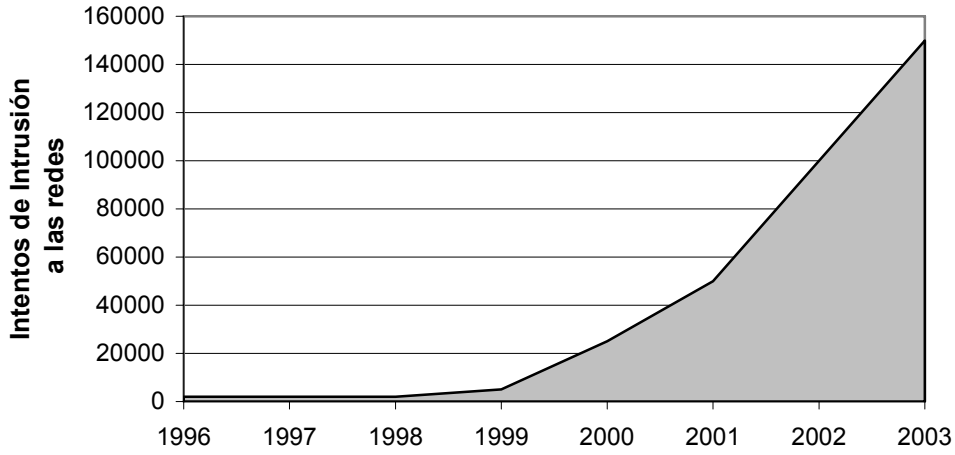


Figura 1.2 - Tendencia de ataques a las redes[2]

Desafortunadamente si bien ha habido importantes avances en el campo, aún existen muchos problemas los cuales será necesario corregir si se desea combatir el crecimiento de intrusiones. Uno de los principales problemas que se vive no sólo en nuestro país sino en diversas partes del mundo es el hecho que la gente que realiza sistemas especializados y de uso particular para las organizaciones, ya sean inventarios o nóminas por ejemplo, no toman en cuenta implementar medidas de seguridad en el software correspondiente o bien tiene una baja prioridad, por lo que esto se ha llegado a traducir en pérdidas económicas para quienes contratan estos servicios, ya sea por problemas inherentes al sistema o factores humanos.

Otro problema radica en que una gran parte de las personas encargadas de proporcionar servicios de seguridad se enfocan en atacar un problema en específico, cuando la realidad indica que se debe abarcar un gran espectro para encontrar las causas de las diversas dificultades que debe combatir el administrador de la red en una empresa. Otro importante factor es que los dueños de corporativos no son conscientes del peligro que significan las intrusiones a sus

[2] Fuente: CERT/CC

redes y es cuando aparece una situación bastante complicada, en la cual se busca ampliar el uso de las comunicaciones pero se ignoran los riesgos que esto contrae.

Las empresas deben ser conscientes cada vez más que la inversión en la seguridad informática es una necesidad creciente, por lo que es pertinente a su vez contar con personal calificado, el cual se enfrenta con nuevos retos ya que actualmente existe una gran cantidad de información que es indispensable conocer si se desea combatir las amenazas que afectan a las compañías. Por consiguiente ya no es posible tener a una sola persona que esté encargada de todas las áreas de informática, debe buscarse gente especializada que pueda brindar la atención requerida a un sector en específico.

El nuevo reto es crear conciencia de lo que significa invertir en servicios de seguridad informática y tener gente capacitada que pueda entender las necesidades de las organizaciones y de los usuarios que hacen uso de los servicios de comunicación, ya que finalmente la tecnología debe estar para facilitar el trabajo del ser humano.

De este modo, es necesario contar con personas que se encarguen adecuadamente de los problemas concernientes a la seguridad informática que además de conocer sobre el funcionamiento de los sistemas computacionales comprendan el problema que representan las vulnerabilidades y amenazas que surgen cada día.

1.2.- El modelo OSI

El modelo OSI (Open System Interconnection) surgió como una necesidad en los años ochenta como una forma de estandarizar los diferentes protocolos de conexión a red que habían tenido un enorme crecimiento en la época. Debido a diversos problemas de incompatibilidad, la Organización Internacional para la Estandarización (ISO) hizo estudios sobre diversos modelos de conexión a fin de

definir una serie de reglas generales que ayudaran a los fabricantes a crear redes compatibles entre sí.

El modelo divide la función de un protocolo en una serie de capas, siendo que cada una cuenta con la característica que sólo puede usar la función de la capa inmediata inferior y sólo puede exportar la funcionalidad propia a la capa inmediata superior, por consiguiente cada uno de los niveles es independiente. De manera típica, las capas inferiores son implementadas en la parte de hardware, y de manera complementaria las capas superiores en software.

El modelo OSI se encuentra dividido en 7 capas o niveles, los cuales son los siguientes:

- Capa de Aplicación
- Capa de Presentación
- Capa de Sesión
- Capa de Transporte
- Capa de Red
- Capa de Enlace
- Capa Física

El flujo de información entre estas capas se muestra en figura 1.3

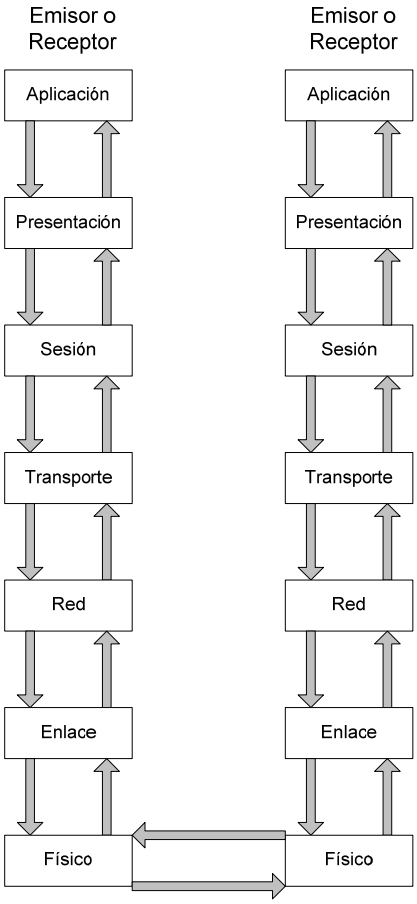


Figura 1.3 – Flujo de datos entre niveles

Los paquetes de datos suelen recibir distintos nombres dependiendo del nivel de fragmentación que tengan. En la capa física se habla de cadenas de bits, en la de enlace se habla de tramas; en la capa de red, de paquetes o datagramas; y en las capas de transporte de segmentos.

1.2.1.- Capa Física

Esta capa define las especificaciones eléctricas y materiales necesarias para la transmisión. Así mismo activa las funciones que administran el enlace físico entre sistemas finales, como son repetidores, hubs o las diversas variedades de la capa física de Ethernet.

En esta parte se modulan los datos digitales para que sean transmitidos por el canal de comunicación usando una señal correspondiente. Por consiguiente busca garantizar la conexión y la transmisión del flujo de bits de tal manera que lo enviado por el emisor llegue sin alteración al receptor.

En este nivel la conexión es básica, por lo que los bits transmitidos sólo pueden ser reconocidos más no existe la capacidad para que puedan ser interpretados.

1.2.2.- Capa de Enlace

La capa de enlace es la encargada de establecer los procedimientos para la transferencia de datos entre equipos de red así como detectar y corregir posibles errores ocurridos en la transmisión a través de la capa física. Ejemplos de protocolos que se desarrollan en esta capa son HDLC y Ethernet en su capa lógica. Es en este nivel en el que los switches y los puentes trabajan.

En algunas redes como las de cobertura local, se suele dividir esta capa en dos subcapas, la primera, LLC (Logical Link Control), la cual actúa con banderas de reconocimiento, detección y retransmisión de tramas. La segunda, MAC (Media Access Control), controla el acceso al medio físico por parte de los dispositivos que estén compartiendo el medio de transmisión, usualmente utilizando el protocolo CSMA/CD, el cual disminuye el número de colisiones. Así mismo, esta subcapa evita la duplicidad de las tramas, utilizando el formato mostrado en la figura 1.4:

7	1	266	266	2	0-1500	0-46	4
Preámbulo	Delimitante de Inicio	Dirección de Inicio	Dirección de Origen	Longitud	DATOS	Relleno	CRC 32

Figura 1.4 – Formato de la trama de datos.
En la parte superior se indica el número de bits correspondiente.

Con lo cual se establece el destino de los datos y se tiene un control de redundancia cíclica para poder tener la certeza de que los datos llegaron correctamente al receptor.

1.2.3.- Capa de Red

El objetivo de este nivel es proporcionar la ruta óptima para los paquetes de datos, para los cuales se utilizan algoritmos de encaminamiento. Del mismo modo puede reportar errores durante la entrega de los paquetes. El ejemplo más conocido de éste nivel es el protocolo IP.

Loa algoritmos que pueden usarse en la capa de red se dividen en dos categorías:

- Estáticos – La ruta queda determinada desde el momento de la instalación de la red, por lo que los equipos encaminadores también llamados routers no basan las decisiones en el estado presente de la red, sino en la configuración original de los nodos.
- Dinámicos – Los encaminadores toman decisiones basándose tanto en las condiciones actuales de la red así como en las actualizaciones periódicas de la red, por lo que si algún enlace deja de estar funcionando en un momento determinado, el algoritmo redireccionará los paquetes ante esta condición.

Por otra parte, en esta capa los paquetes son segmentados para su transmisión en unidades más complejas, en las cuales se asignan direcciones lógicas del receptor, y del mismo modo, los paquetes son reensamblados en el nodo destino.

1.2.4.- Capa de Transporte

La función de esta capa es el transporte de datos entre usuarios finales a través de la red. Podemos hacer cierta analogía entre la capa de enlace y la capa de transporte ya que ambas se encargan de la gestión de las tramas, por lo que podemos decir que la capa de transporte es a las redes amplias lo que la de enlace es a las redes locales.

Para llevar a cabo el transporte de los datos entre los distintos nodos de la red, se establecen circuitos virtuales que son los encargados de proporcionar un servicio confiable por medio de un sistema de detección y recuperación de errores. Los ejemplos más reconocidos de esta capa se encuentran en los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

Algunas de las funciones de esta capa incluyen la adhesión de controles de integración entre los usuarios de la red a fin prevenir pérdidas de datos, control de flujo de transacciones y el direccionamiento de procesos de máquina a procesos de usuario, fragmentación y reensamblado de datos y garantía de transferencia de información a través de la red.

1.2.5.- Capa de Sesión

Este nivel es el encargado de establecer el diálogo entre computadoras. Como su nombre lo indica, es la parte responsable de iniciar, mantener y finalizar las sesiones entre receptor y emisor. Así mismo, también es en esta capa que se realiza la obtención de registros de problemas de sesión.

La principal función de la capa de sesión es poder manejar problemas de sincronización y asegurar que no exista inconsistencia en los datos. Para tales fines utiliza transmisiones full duplex o half duplex y establece checkpoints, los

cuales actúan como puntos de referencia durante la transferencia de datos que se utilizan para la recuperación de sesiones perdidas.

1.2.6.- Capa de Presentación

Esta capa proporciona los servicios a la capa de aplicación garantizando que los datos recibidos puedan ser interpretados y utilizados por dicha capa. Por lo tanto se encarga del argumento sintáctico de los datos, es decir, el formato en que los datos son transmitidos. Un ejemplo del servicio prestado por la capa de presentación es la conversión de código ASCII, el cual es utilizado por diversas aplicaciones, a un formato común que pueda ser enviado por la red.

Otra tarea que normalmente se realiza en este nivel es el cifrado y descifrado de los datos, aunque puede ser realizado en alguna de las capas adyacentes, del mismo modo, en esta capa se realiza la compresión de los datos.

1.2.7.- Capa de Aplicación

Es la capa que provee el modelo para que el usuario pueda acceder a la información en la red, es decir, permite la interacción entre el usuario y la red por medio de las aplicaciones correspondientes. Algunos ejemplos de aplicaciones son FTP, SSH, POP3, SMTP, etcétera.

La capa de aplicación permite establecer la disponibilidad de diversos elementos que deben participar en la comunicación, sincronizando las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de integridad de los datos.

1.3.- Principios de Seguridad

En las organizaciones se emplean una gran variedad de tecnologías de la información los cuales a su vez utilizan una gran diversidad de usuarios. La seguridad en dichas tecnologías representa entonces un asunto de vital importancia ya que de éstas dependen la integridad y la supervivencia de las empresas.

La Seguridad de la Información (conocida como INFOSEC por sus siglas en inglés), es un proceso en constante cambio, que actúa de manera dinámica de acuerdo a las necesidades del momento y se encuentra en constante evolución.

Las amenazas a las tecnologías de la información avanzan a la par con los nuevos descubrimientos, por lo que la seguridad en dicho rubro debe garantizar que los activos más importantes se encuentren protegidos.

Un primer paso para comenzar a proteger los sistemas de información es conocer los principios de la seguridad de la información, algo que cualquier organización debe tener en cuenta con el fin de proteger a sus redes, ya que conforme ha avanzado el tiempo los sistemas se han vuelto cada vez más vulnerables a intrusiones y es entonces que se vuelve necesario conocer las principales características de la protección a las redes.

1.3.1.- Ciclo de vida de la seguridad de la información

El modelo de ciclo de vida de INFOSEC está basado en la protección de los activos y en la administración de riesgos, amenazas y vulnerabilidades. En la figura 1.4 se puede observar la representación de este ciclo por medio de un círculo externo, otro interno y en el interior los activos de la organización.

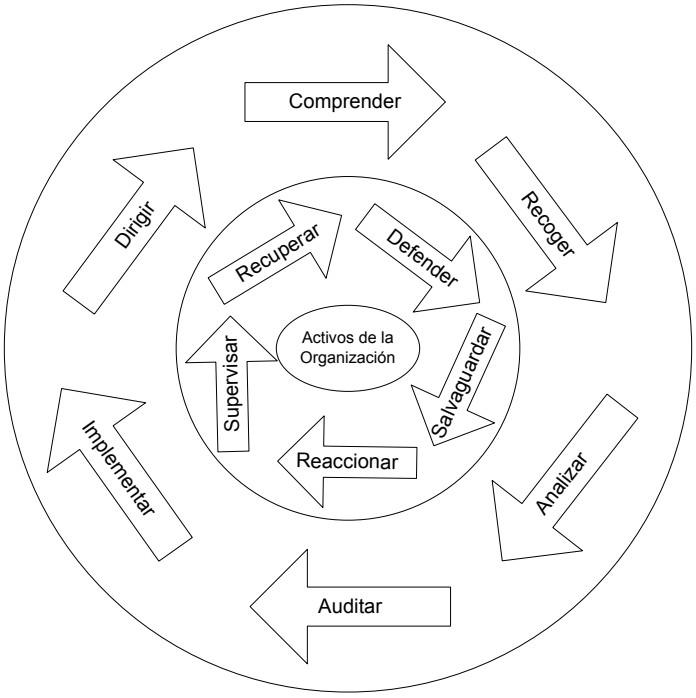


Figura 1.4 – Modelo del proceso de seguridad basado en riesgos y activos [3]

El círculo externo abarca el proceso global de la seguridad, tanto a nivel operacional como a nivel directivo. Trabaja de manera independiente al movimiento del círculo interno, pero de manera estrecha con éste mismo, el círculo externo es vital para definir el programa de administración de riesgos de las organizaciones. El círculo interno está conformado por controles de acción.

Ambas ruedas representan un proceso continuo, por lo que para garantizar la eficacia de la seguridad de la información debe existir una actualización constante de los procesos y realizar una valoración completa de los riesgos, a fin de mantener funcionando eficientemente los sistemas.

La seguridad de la información actualmente es inherente y necesaria, aunque no es hermética y por lo tanto es perfectible Por lo que no es posible eliminar todos los riesgos ni evitar el uso inapropiado de la información. Entonces el nivel de seguridad de la información debe ser acorde al valor de la pérdida de dicha

[3] HORTON Mike, MUGGE Clinton, "Claves Hackers", Ed. Mac Graw Hill/Interamericana de España, 2004, pp. 5

información, tanto en el aspecto financiero como en el ámbito del impacto en el prestigio de la organización correspondiente.

1.3.2.- Protección a redes

Existen diversos mecanismos de defensa y protección en torno a las redes. Los principales propósitos de salvaguardar los activos y mantener los controles de seguridad, los cuales se pueden resumir en:

- Proteger
- Detener
- Responder
- Recuperar

En esencia el concepto de seguridad se basa en la cantidad de tiempo y la cantidad de recursos necesarios para que una amenaza pueda llegar a comprometer a uno o varios de los activos, dada una o más vulnerabilidades presentes en el sistema informático.

Existen diversos niveles de profundidad en cuanto a medidas preventivas se refiere. El siguiente listado muestra una serie de ejemplos que en combinación pueden satisfacer de manera eficiente la necesidad de protección a los sistemas de información, aunque es responsabilidad del administrador definir puntualmente las necesidades de la empresa:

- Cuentas de usuarios confiables.
- Cuentas de administradores confiables y de acceso remoto protegido.
- Protección contra virus y programas maliciosos.
- Actualización de software.
- Medidas preventivas en contra de descuidos por parte de los usuarios.

- Medidas en contra de usurpación de identidades y fuga de información.
- Protección contra el robo físico de equipos.

La seguridad de la información se basa en tres principios fundamentales conocidos como CIA por sus siglas en inglés (Confidentiality, Integrity, Availability) con los cuales podemos determinar los principales activos que deseamos proteger dentro de una empresa:

Confidencialidad – Es necesario implementar las medidas de seguridad necesarias, que garanticen que la información sólo se encuentre disponible para aquellos que tengan necesidad de consultarla. Los datos deben contar con medidas estrictas para controlar y en un caso dado, impedir el acceso a ésta por personal no autorizado.

Integridad – Resulta vital garantizar que los datos sean fiables y que no hayan sido modificados sin previa autorización. La integridad resulta crítica cuando los datos se utilizan para llevar a cabo transacciones, análisis estadísticos o cálculos matemáticos, en los cuales la precisión de las cifras manejadas es de carácter crítico.

Disponibilidad – Implementar las medidas de seguridad para garantizar que los datos sean accesibles en el momento en el que se necesiten. La disponibilidad puede resultar de crítica importancia cuando se tenga que acceder a los datos o a las aplicaciones en tiempo real.

En la tabla de la figura 1.5 se muestra una clasificación de riesgos de acuerdo a estos tres aspectos, tomando como referencia cuatro activos que usualmente son los más comunes dentro de las organizaciones y que podemos encontrar usualmente dentro de una red empresarial.

Elemento	***Confidencialidad***	***Integridad***	***Disponibilidad***
Hardware	Acceso al equipo.	Modificación de sus partes.	Robo o utilización de equipos eliminando el servicio.
Software	Copias no autorizadas del software.	Alteración de un programa para que falle durante la ejecución y/o realice alguna tarea no pretendida.	Borrado de programas, denegación del acceso.
Datos	Lectura de datos no autorizada.	Modificación de archivos existentes o creación de nuevos.	Borrado de archivos, denegando el acceso.
Líneas de Comunicación	Lectura de mensajes, observación del tráfico de mensajes desde y hacia una máquina.	Mensajes modificados, retardados, reordenados o duplicados, generación de mensajes falsos.	Destrucción o eliminación de mensajes lo cual implica redes no disponibles.

Figura 1.5 – Clasificación de riesgos por elementos del sistema

1.3.3.- Administración de riesgos

Podemos definir a la administración de riesgos como una serie de prácticas y procesos a través de los cuales se neutralizan los riesgos y amenazas a través de las medidas correspondientes de tal modo que no se interfiera, se trastorne o se perjudiquen las actividades de la organización. A través de la administración de riesgos se busca tomar las mejores decisiones referentes a la protección de los activos y ayuda a determinar un plan de acción en el que se basará la seguridad de la información organizacional.

Una vez que se han realizado los estudios correspondientes al análisis de riesgos, es mucho más sencillo determinar el valor justo de los activos críticos, así como de las posibles amenazas y vulnerabilidades que se pudieran detectar. Para tales fines es necesario conocer tanto cuantitativa como cualitativamente los aspectos mencionados, siendo la valoración de riesgos la herramienta que más utilizada para este fin.

Podemos dividir la valoración de riesgos en cinco rubros: valoración de los activos críticos, de las amenazas, de las vulnerabilidades, análisis de riesgos y resolución de riesgos. Estos dos últimos son un estudio pertenecientes a la valoración de riesgos referentes a la totalidad de los procesos implicados.

La valoración de activos críticos en primera instancia a los activos y posteriormente los califica a partir de un análisis de diversas variables. Se puede establecer una lista inicial con todos los activos que se tengan, y posteriormente ir reduciendo este listado basándose en la importancia dentro de un contexto determinado. Una vez que se tiene una lista final de activos críticos, se realiza el análisis basándose en los siguientes aspectos:

- Criticidad de los datos.
- Criticidad de la misión.
- Criticidad organizativa.
- Dificultad en su sustitución o recuperación.

La valoración de las vulnerabilidades es un estudio que se encarga de identificar las debilidades inherentes de los activos así como el entorno que los rodea. Si bien, las vulnerabilidades se basan principalmente en aspectos tecnológicos, se deben incluir aspectos de control de procedimientos operativos. Se recomienda que las valoraciones en un mismo entorno se realicen al mismo tiempo, así como las siguientes recomendaciones:

- Revisión de la estructura de la red.
- Revisiones de procedimientos y políticas.
- Revisiones de aplicaciones en línea.
- Revisión de seguridad física.

La valoración de amenazas se refiere a la identificación de factores que pueden causar daño a los activos, ya sea de manera inmediata o de forma potencial. Así

mismo, se determina el nivel de severidad que conllevan los daños. Los principales aspectos que se consideran dentro de las amenazas son:

- Probabilidad de ocurrencia.
- Probabilidad de éxito.
- Impacto en términos de daños.

Las amenazas con una baja probabilidad de ocurrencia, no resulta necesario que sean consideradas. Así mismo se debe establecer la relación entre las vulnerabilidades detectadas y las amenazas encontradas.

El análisis y la resolución de riesgos se encuentran estrechamente relacionados y describen un proceso sistemático de análisis de los resultados obtenidos durante la valoración de los activos, vulnerabilidades y amenazas. Los aspectos que se deben tomar en cuenta para poder determinar los diversos niveles de riesgo son:

- El valor del activo, ya sea tangible o intangible, que se ha determinado durante el proceso de valoración correspondiente.
- Amenazas y su nivel asociado.
- Vulnerabilidades y su nivel asociado.

El desarrollo de la administración de riesgos deriva de manera importante en las políticas de seguridad, las cuales definen de manera clara y formal qué se considera valioso para la empresa y especifican qué medidas se deben tomar para proteger los activos; por lo que se escriben para:

1) Aclarar qué se protege y porqué.
2) Establecer la responsabilidad de la protección.
3) Poner las bases para resolver conflictos posteriores.

Por consiguiente, es necesario un compromiso profundo por parte de la organización para identificar y establecer las fallas y debilidades dentro de sí misma, así como procurar la actualización y renovación con el fin de lograr adaptarse a constantes cambios.

Capítulo 2

Políticas de Seguridad

Capítulo 2
Políticas de Seguridad

La principal preocupación de los ejecutivos y dueños de organizaciones son los virus informáticos, como se demuestra un estudio de percepción referente a la seguridad informática realizado en México durante el 2007 (figura 2.1), aunque la realidad nos indica que el fraude es la actividad con mayor riesgo dentro de las empresas. Por lo tanto, las inversiones que se destinan a seguridad sólo aparecen después de que ha surgido un problema serio dentro de la organización.

A. Virus
B. Pérdida de la información
C. Invasión a la privacidad
D. Compras en línea / uso de banca electrónica
E. Confidencialidad de la información
F. Integridad de la información
G. Robo de Identidad
H. Hackers y otros agresores externos
I. Extracción de información
J. Spyware / Adware
K. Software deficiente
L. Phishing / Ingeniería Social
M. Spam
N. Insuficiencia de estructura de seguridad (equipo / software)
O. Desconocimiento

Figura 2.1 – Principales preocupaciones relacionadas a la seguridad informática[4]

[4] Fuente: Joint Future System, S.C.

No sólo se debe considerar la amenaza que representan los virus, ya que una inadecuada utilización del sistema o la pérdida de la confidencialidad son factores perjudiciales dentro de las redes. Existe también un agente menos obvio y que causa costo económico dentro de las organizaciones, el spam. El envío de correos electrónicos masivos pone en riesgo el crecimiento dentro de un negocio produciendo la degradación del servicio.

Los principales problemas radican en la falta de conciencia de los usuarios finales, las limitaciones tanto de presupuesto como de personal especializado, así como el acelerado cambio en la tecnología son los principales obstáculos a los que hay que enfrentar. Por éstas razones surgen las políticas de seguridad informática, siendo una herramienta laboral que tiene como finalidad crear conciencia en quienes colaboran dentro de una organización.

Podemos entonces definir a las políticas de seguridad como el conjunto de normas y procedimientos documentados y comunicados, que tienen por objetivo minimizar los riesgos informáticos e involucra el uso de herramientas y el cumplimiento de actividades por parte del personal. Por consiguiente, las políticas de seguridad deben ser concernientes a todos los que conforman la organización a fin de que resulten efectivas para el cumplimiento de los objetivos planteados durante su creación.

2.1.- Estructura de la Seguridad Informática

La historia de la seguridad informática se remonta desde que existieron los primeros documentos escritos. Uno de los primeros registros que se tiene de la utilización de códigos para cifrar la información escrita se encuentra con los egipcios hace dos mil años. Posteriormente, civilizaciones como la de Babilonia, Mesopotamia y Grecia inventaron formas de proteger su información escrita.

La codificación de la información ha sido utilizada principalmente durante periodos de guerra, incluyendo por supuesto las dos guerras mundiales. Una de las máquinas de codificación mejor conocidas fue “Enigma”, utilizada por los alemanes para crear mensajes codificados en la Segunda Guerra Mundial.

En los últimos veinte años, la importancia de la seguridad informática se ha puesto de manifiesto debido a diversos casos. Una de los más destacados fue la del “Gusano de Internet” en 1988, que se extendió por decenas de miles de computadoras como resultado de una investigación realizada por el profesor Robert Tappan Morris.

En años recientes el avance de las comunicaciones ha hecho necesaria la seguridad informática cuyo objetivo principal es la protección de los recursos informáticos, en los cuales se incluyen los equipos, los medios de almacenamiento, el software y en general la información. Una sólida estructura de la información se basa en cuatro puntos fundamentales:

1. -Estrategias de administración para la seguridad informática y en políticas de seguridad que servirán para comunicar las estrategias de protección correspondientes a la organización.

2. -Monitorización de los eventos, es decir, tener procesos reactivos que permitan al administrador tener una métrica con la cual poder medir la efectividad en la implantación de ciertas políticas específicas y poder identificar la necesidad de cambios en las mismas.

3. -Administración de cambios y establecimiento de controles desarrollando procesos que se dirijan a programas de capacitación del personal.

4. -Tecnologías de la información necesarias para proveer la protección apropiada y el soporte necesario para los diversos procesos involucrados en la organización.

Así, destaca que entre las tecnologías de protección más utilizadas en la actualidad se encuentra el control de accesos, es decir el uso de contraseñas, el software antivirus y la implementación de firewalls. De la misma manera "los ataques más comunes durante los últimos años fueron los virus informáticos, el spamming de correo electrónico y la denegación de servicios."[5]

2.1.1.- Estándar ISO 17799

ISO 17799, es el único estándar existente que ofrece un punto de referencia para poder constituir mecanismos de seguridad informática. El estándar puede ser aplicado a todo tipo de organizaciones, y es solicitado obligatoriamente en aquellas empresas que requieren contar con fuertes mecanismos de seguridad, siendo que también puede ser utilizado como una herramienta de mercadeo a fin de poder ofrecer a los clientes un aval de calidad.

Existen diversos beneficios tanto para los clientes como para las organizaciones que siguen los lineamientos planteados por el estándar ISO 17799, especialmente porque en la actualidad ha surgido una enorme dependencia de los recursos relacionados a la información y los que son objeto de diversos tipos de amenazas. Por consiguiente, podemos asegurar que "una empresa certificada tendrá en cuenta lo siguiente:

- Mayor seguridad en la empresa.
- Planeación y manejo de la seguridad más efectivos.
- Alianzas comerciales y comercio electrónico más seguros.

[5] Fuente: Centro de Investigación en Seguridad Informática Argentina

- Mayor confianza en el cliente.
- Auditorías de seguridad más precisas y confiables.
- Menor responsabilidad civil"[6]

El estándar ISO 17799 se divide en diez secciones de seguridad, las cuales son utilizadas como base para determinar riesgos y poder establecer controles de éstos mismos. Las secciones son:

Parte 1 – Política de seguridad

La política de seguridad es un conjunto de reglas y prácticas que regulan la manera de dirigir, proteger y distribuir los recursos de una organización, y es a través de dicha política que se definen las propiedades de seguridad con las que un sistema debe contar.

El objetivo es proporcionar una base con la cual se puedan establecer las medidas de seguridad adecuadas en lo referente al acceso a terceros a la información, así como la administración de la seguridad dentro de las organizaciones y el establecimiento de las condiciones para la implementación la misma.

Parte 2 – Seguridad de la organización

Dentro del marco de las organizaciones, se debe establecer en que manera va a ser manejada la seguridad de la información, así como la metodología que se planteará para establecer la manera en que se mantendrá, el tratamiento que la información tendrá y la manera en ésta será organizada, no sólo en refiriéndose a quienes laboran dentro de la organización, sino también al personal externo que pudiera tener acceso a la misma.

[6] LÖPEZ Barrientos María Jaquelina, QUEZADA Reyes Cintia, "Fundamentos de Seguridad Informática" Universidad Nacional Autónoma de México, México, p.66

La segunda parte de la ISO 17799 nos hablas sobre los siguientes puntos al momento de establecer la seguridad de la organización:

- Foro para el manejo de la seguridad de la información.
- Coordinación del sistema de seguridad de la información.
- Responsables de la seguridad de la información.
- Procesos de autorización.
- Especialista en seguridad de la información.
- Cooperación administrativa.
- Análisis independiente.
- Acceso de la tercera entidad.
- Outsourcing.

Parte 3 – Clasificación y Control de Activos

Ésta sección busca definir diversos niveles de protección y medidas de tratamiento para cada uno de los activos de acuerdo a su clasificación, los cuales se basan en la criticidad y en la sensibilidad de los datos, así como el establecimiento de las responsabilidades correspondiente de cada uno de los dueños de los activos.

Los mecanismos utilizados para mantener el control son la realización de inventarios, los cuáles ayudan a establecer a su vez que niveles de protección resultan adecuados para el manejo de los activos.

Parte 4 – Seguridad del Personal

La seguridad personal se enfoca en reducir el error humano así como los actos ilícitos con la finalidad de evitar el uso inadecuado de equipos y asegurarse que los usuarios tengan conocimiento de las amenazas de seguridad, además de buscar el respaldo de todos aquellos que laboran dentro de la organización para la aplicación de la misma

Por otra parte también es necesario establecer medios de comunicación con el personal a fin de determinar las debilidades existentes en el sistema, haciendo del conocimiento del empleado sus responsabilidades concernientes a la seguridad de la información. En éste ámbito es necesario dar capacitación tanto al personal nuevo como al ya establecido, en base a las políticas de seguridad de la organización.

Parte 5 – Seguridad Física y Ambiental

Es necesario mantener los activos en áreas seguras y protegidas a fin de evitar factores que podrían perjudicar el correcto funcionamiento del equipo que contiene información sensible, del mismo modo es necesario establecer barreras de seguridad que protejan al equipo de intrusiones previniendo daños e interferencias a las comunicaciones.

Asimismo, además de las protecciones establecidas para el acceso de las áreas restringidas, es necesario resguardar los equipos durante traslados y su permanencia en áreas que no se encuentren protegidas, siendo en estos casos necesario siempre contar de manera estricta con la autorización de la administración

Parte 6 – Gestión de Comunicaciones y Operaciones

El objetivo es asegurar la operación correcta y segura de los recursos concernientes al procesamiento de la información así como contar con respuestas inmediatas a posibles incidentes. Por consiguiente se busca evitar la interrupción de las actividades económicas, previniendo la pérdida, la modificación, o que se de un mal uso de la información intercambiada entre las organizaciones.

El manejo de incidentes se basa en dar una respuesta efectiva ante cualquier incidente, es por eso que resulta de vital importancia establecer de manera clara y precisa responsabilidades y procedimientos, que permitan dar respuesta a los diversos problemas que se presenten. Por otra parte, es necesario contar con una metodología a seguir en los casos de actualizaciones y cambios del sistema, a fin de poder garantizar la continuidad de los servicios.

Parte 7 – Control de Accesos

Entre los principales ejes de éste apartado se encuentran controlar los accesos entre la red perteneciente a la organización y las redes externas, para lo cuál se realizaran registros y revisión de los eventos de las actividades en las redes con la finalidad de prevenir accesos no autorizados a los sistema de información o bien, detectar actividades no autorizadas por la administración.

En primera instancia es necesario conocer los requerimientos de la organización, a fin de establecer las medidas necesarias para establecer diferentes niveles de acceso, así como los privilegios a los diferentes activos de la empresa. El uso de contraseñas resulta importante en la administración de los usuarios, es un modo práctico de controlar la asignación de privilegios y en consecuencia la seguridad en el aspecto de autenticación de usuarios legítimos. Otro punto, es la seguridad en el acceso a los sistemas operativos, de los cual podemos destacar los siguientes mecanismos:

- Inicio de sesión segura.
- Identificar automáticamente terminales
- Establecer tiempo de espera de terminal para el usuario y/o la conexión.
- Autenticar usuarios.
- Manejar contraseñas.
- Asegurar utilidades del sistema.

- Suministrar a los usuarios funciones de emergencia contra el encierro como "botones de pánico"

Parte 8 – Desarrollo y Mantenimiento de Sistemas

Ésta etapa es referente a la definición de los procedimientos que se llevarán a cabo durante el ciclo de vida de los sistemas, así como en la infraestructura en la que se soportan. Del mismo modo deben existir controles de seguridad y validación en los datos en el desarrollo de los sistemas de información.

Los requerimientos definidos durante el desarrollo y la consecución de las aplicaciones sirven para evitar la pérdida de la información, así como para prevenir el mal uso de los recursos de los mismos. Para tales fines deben existir controles adicionales para los sistemas que procesan, como son el uso de la criptografía para proteger la confidencialidad de los sistemas, o bien mantener la integridad de los sistemas por medio de controles de acceso.

Parte 9 – Plan de continuidad del negocio

La continuidad del negocio trata sobre la capacidad de la organización para combatir las interrupciones de las operaciones normales, realizar el análisis de las consecuencias que puede traer la interrupción de los servicios y en los casos que se hayan presentado algún tipo de contingencia relacionada con éste aspecto, tomar las medidas correspondientes para evitar hechos similares en el futuro.

Para llevar a cabo los objetivos planteados se debe asegurar la coordinación del personal del la organización a fin de que se encuentren preparados en caso de alguna contingencia, asignando responsabilidades para cada una de las actividades definidas. Por otra parte deben realizarse pruebas que permitan asegurar que en la práctica los sistemas son actuales y eficaces.

Parte 10 – Cumplimiento

La última sección se refiere a la capacidad que debe tener la organización para asegurar la conformidad entre los sistemas de seguridad y las políticas de seguridad, a fin de maximizar la eficiencia y reducir la interferencia externa a los procesos de los sistemas.

Se debe realizar una revisión de la seguridad de los sistemas de información periódicamente con el fin de garantizar el cumplimiento de las políticas de seguridad, el cumplimiento de los requerimientos legales, la verificación de los requerimientos técnicos planteados por la administración así como determinar los plazos de actualización de las políticas.

2.1.2.- Criterios Comunes (CC)

A nivel mundial se ha establecido una norma de seguridad llamada “Criterios Comunes” (CC), la cual sirve para evaluar la seguridad de los productos relacionados con la tecnología de la información, y establecer los parámetros para definir y regular reglas de seguridad informática abarcando diversos aspectos, desde definir el análisis para establecer las políticas de seguridad informática hasta el planteamiento de las garantías correspondientes.

Debido a que CC son un medio para definir la medida de los aspectos de la seguridad de los productos de tecnologías de la información, estos establecen criterios para facilidad de ejecución de pruebas, indicando problemas de seguridad, soluciones a los mismos y determinar por parte de los evaluadores qué es lo que el producto hace.

La norma está conformada de tres partes principales

- Introducción y modelo general

- Requerimientos de seguridad funcional
- Requerimientos de garantía de seguridad

La primera parte se refiere a cómo fueron establecidos los criterios comunes y para quiénes están destinados. También describe la definición de funcionalidad de seguridad, los requisitos de confiabilidad y la estructura a seguir de protección así como las metas de seguridad.

La segunda parte se enfoca en los requerimientos funcionales de los usuarios y desarrolladores. Se organizan en once clases, denominadas clases de requerimientos y cada una cubre un área específica del campo de la seguridad, las cuáles a su vez se dividen en diversas familias funcionales que describen de manera específica a los diferentes aspectos que conforman a la clase correspondiente.

Las operaciones manejadas en esta parte de la norma son: iteración, un componente es usado en varias operaciones; asignación, especificación de un parámetro en particular; selección, determinación de un elemento de la lista; y refinamiento, referente a la adición de detalles. Las clases con sus familias correspondientes son las siguientes:

1.- Clase FAU: Auditoria de la seguridad.

FAU_ARP – Respuesta automática de auditoria de seguridad.
FAU_GEN – Generación de datos de auditoria de seguridad.
FAU_SAA – Análisis de auditoria de seguridad.
FAU_SAR – Revisión de la auditoria de seguridad.
FAU_SEL – Selección del evento de auditoria de seguridad.
FAU_STG – Almacenamiento del evento de auditoria de seguridad.

2.- Clase FCO: Comunicación.

FCO_NRO – No repudio de origen.

FCO_NRR – No repudio de receptor.

3.- Clase FCS: Soporte de cifrado.

FCS_CKM – Administración de claves de cifrado.

FCS_COP – Operación de cifrado.

4.- Clase FDP: Protección de datos de usuario.

FDP_ACC – Política de control de accesos.

FDP_IFC – Política de control de flujo de información.

FDP_ACF – funciones de control de acceso.

FDP_IFF – Funciones de control de flujo de información.

FDP_ITT – Transferencia TOE (Target Of Evaluation) interna.

FDP_RIP – Protección de información residual.

FDP_ROL – Retroceso.

FDP_SDI – Integridad de los datos almacenados.

FDP_DAU – Autenticación de datos.

FDP_ETC – Exportación al exterior del control de las funciones de las funciones de seguridad del objeto de evaluación.

FDP_ITC – Importación del exterior del control de las funciones de seguridad del objeto de evaluación.

FDP_UCT – Protección de transferencia de confidencialidad de datos de usuario entre funciones de seguridad del objeto de evaluación.

FDP_UIT – Protección de transferencia de integridad de datos de usuario entre las funciones de seguridad del objeto de evaluación.

5.- Clase FIA: Identificación y autenticación.

FIA_AFL – Fallas de autenticación.

FIA_ATD – Definición de atributos de usuario.

FIA_SOS – Especificaciones de secretos.

FIA_UAU – Identificación de usuario.

FIA_USB – enlace usuario-sujeto.

6.- Clase FMT: Administración de la seguridad.

FMT_MOF – Administración de funciones en TSF.

FMT_MSA – Administración de atributos de seguridad.

FMT_MTD – Administración de datos de las funciones de seguridad del objeto de evaluación.

FMT_REV – Revocación.

FMT_SAE – Vigencia de atributos de seguridad.

FMT_SMR – Perfiles de administración de seguridad.

7.- Clase FPR: Privacía

FPR_ANO – Anonimato.

FPR_PDE – Pseudonimia.

FPR_UNL – Imposibilidad de asociación.

FPR_UNO – Inobservabilidad.

8.- Clase FPT: Protección de las funciones de seguridad del objeto de evaluación.

FPT_AMT – Prueba de la máquina abstracta subyacente.

FPT_FLS – Seguro ante fallas.

FPT_ITA – Disponibilidad de datos exportados de las funciones de seguridad del objeto de evaluación.

FPT_ITC – Confidencialidad de datos exportados de las funciones de seguridad del objeto de evaluación.

FPT_ITI – Integridad de datos TSF exportados.

FPT_ITT – Transferencia interna de datos objeto de evaluación-funciones de seguridad.

FPT_PHP – Protección de las funciones de seguridad del objeto de evaluación.

FPT_RCV – Recuperación confiable.

FPT_RPL – Detección de retransmisión.

FPT_RVM – Mediación de referencia.

FPT_SEP – Separación de dominio.

FPT_SSP – Protocolo de sincronía de estado.

FPT_STM – Sellos de tiempo.

FPT_TDC – Consistencia de datos de funciones de seguridad entre funciones de seguridad.

FPT_TRC – Consistencia de retransmisión de datos de funciones de seguridad dentro del objeto de evaluación.

FPT_TST – Autoverificación de las funciones de seguridad del objeto de evaluación.

9.- Clase FRU: Utilización de recursos.

FRU_FLT – Tolerancia a fallas.

FRU_PRS – Prioridad de servicio.

FRU:RSA – Asignación de recursos.

10.- Clase FTA: Acceso a la TOE (Target Of Evaluation).

FTA_LSA – Limitación en el ámbito de atributos seleccionables.

FTA_MCS – Limitación en sesiones concurrentes múltiples.

FTA_SSL – Cierre de sesión.

FTA_TAB – Banderas de acceso del objeto de evaluación.

FTA_TAH – Historia de acceso del objeto de evaluación.

FTA_TSE – Establecimiento de sesión del objeto de evaluación.

11.- Clase FTP: Caminos/canales confiables.

FTP_ITC – Canal confiable entre funciones de seguridad.

FTP_TRP – Camino confiable

La última parte se enfoca en establecer el criterio de confiabilidad que los evaluadores tendrán para calificar el desempeño de los desarrolladores y sus productos. CC proporciona garantías a través de la investigación activa, la cuál es una evolución del producto o sistema IT para determinar sus propiedades. Se

divide en dos secciones ésta parte de la norma: la primera define la escala de los CC para la clasificar la evaluación obtenida por los productos y se divide en siete clases de evaluación de garantía (Evalution Assurance Level) con sus correspondientes familias:

1.- Clase ACM: Administración de la configuración.

ACM_AUT – Automatización de la administración de la configuración.

ACM_CAP – Capacidades de la administración de la configuración.

SCP – Ámbito de la administración de la configuración.

2.- Clase ADO: Distribución y operación.

ADO_DEL – Distribución.

ADO_IDS – Instalación, generación e inicialización.

3.- Clase ADV: Desarrollo.

ADV_FDP – Especificación funcional.

ADV_HLD – Diseño de alto nivel.

ADV_IMP – Representación de la implantación.

ADV_INT – Funciones de seguridad internas del objeto de evaluación.

ADV_LLD – Diseño de bajo-nivel.

ADV_RCR – Correspondencia de representación.

ADV_SPM – Modelo de política de seguridad.

4.- Clase AGD: Documentos guía.

AGD_ADM – Guía del administrador.

AGD_USR – Guía del usuario.

5.- Clase ALC: Soporte del ciclo de vida.

ALC_DVS – Seguridad de desarrollo.

ALC_FLR – Corrección de fallas.

ALC_LCD – Definición de ciclo de vida.

ALC_TAT – Herramientas y técnicas.

6.- Clase ATE: Pruebas.

ATE_COV – Cobertura.

ATE_DPT – Profundidad.

ATE_FUN – Pruebas funcionales.

ATE_IND – Pruebas independientes.

7.- Clase AVA: Evaluación de la vulnerabilidad.

AVA_CCA – Análisis de canal encubierto.

AVA_MSU – Mal uso.

AVA_SOF – Robustez de las funciones de seguridad del objeto de evaluación.

AVA_VLA – Análisis de vulnerabilidad.

La segunda parte de la última sección se refiere a los niveles de seguridad, proporcionando una escala creciente que compara el nivel de garantía obtenido con el costo y la viabilidad de adquirir dicho grado. Se divide en siete niveles, los cuales se ordenan de manera jerárquica ya que cada uno presenta un grado mayor que los anteriores. Los niveles son:

EAL_1: se refiere a la prueba de funcionalidad y es aplicable donde la confidencialidad en alguna operación es requerida, pero las amenazas de seguridad no son serias.

EAL_2 se refiere a las pruebas estructurales dentro de la organización y provee el aseguramiento del objetivo de seguridad total y una descripción básica de la arquitectura.

EAL_3 se refiere a la realización de pruebas metodológicas, es decir, se realiza el aseguramiento a través del uso de ambientes desarrollados por medio del control de los datos dados.

EAL_4 incluye revisión, pruebas y diseño metodológico, se enfoca a incrementar el aseguramiento por medios más concisos en el diseño, implementando mecanismos mejorados y procedimientos que proveen confidencialidad.

EAL_5 se refiere a diseños y pruebas semi-formales, con lo cuál hay una implementación de una arquitectura mejor estructurada, es decir, más analizable, así como mecanismos de seguridad mejorados.

EAL_6 se refiere al diseño verificado y probado semi-formalmente, siendo que éste nivel representa un gran incremento al aseguramiento con respecto al anterior nivel porque requiere un análisis más comprensivo, una representación estructurada de la implementación y una arquitectura más estructurada.

EAL_ 7 incluye el diseño verificado y probado formalmente, siendo entonces el nivel más alto de acuerdo a las políticas de seguridad con base en la arquitectura estructural derivada del objetivo de seguridad, las cuales deben tener confirmaciones independientes, desarrolladas y analizadas por pruebas de vulnerabilidades a ataques de penetración con un alto potencial de riesgo.

Los beneficios de CC son diversos, podemos mencionar que a los usuarios les proporciona diversas opciones de productos de calidad, además de que facilita la comunicación entre los usuarios y los desarrolladores brindando un esquema que resulta común y comprensible para ambas partes, además de que los productos que han sido evaluados representan confiabilidad para quienes hagan uso de ellos, ya que los criterios comunes son públicos y de carácter independiente.

2.2.- Establecimiento de Políticas de Seguridad

Una política de seguridad puede entenderse como una forma de establecer contacto con los usuarios, ya que en sí mismas establecen la forma en que se debe actuar en relación con los servicios informáticos de la organización. Por consiguiente, las políticas de seguridad son una descripción de lo que se desea proteger, así como los motivos para esto.

Es necesario englobar la visión de cada uno de los miembros de la empresa en donde se quieren establecer las nuevas reglas. Es entonces que se vuelve necesario realizar un balance entre dos aspectos fundamentales relacionados con la seguridad; el primero se refiere a las limitaciones del usuario final al tener establecido un control bastante estricto sobre la red; el segundo aspecto radica en el riesgo que intrusión que se corre con un bajo control.

Ambos aspectos se ilustran en las gráficas de las figuras 2.2 y 2.3 respectivamente:

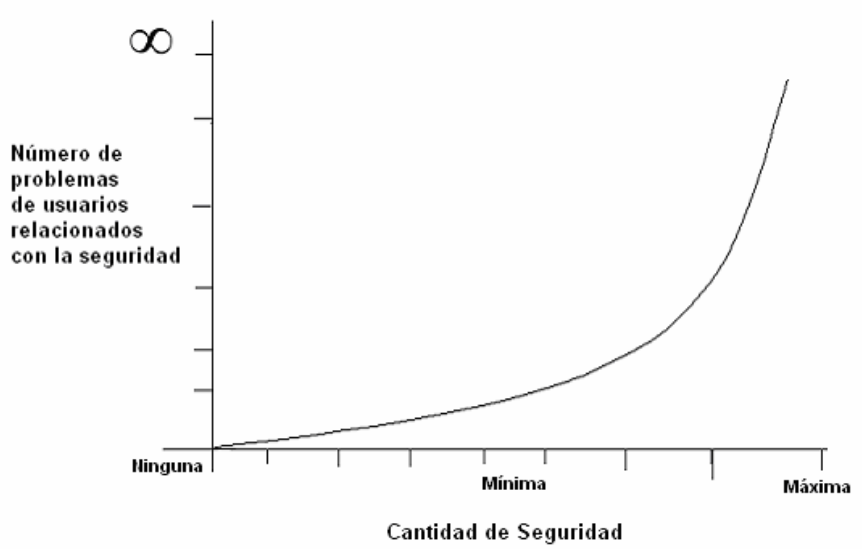


Figura 2.2 – Seguridad contra problemas para los usuarios

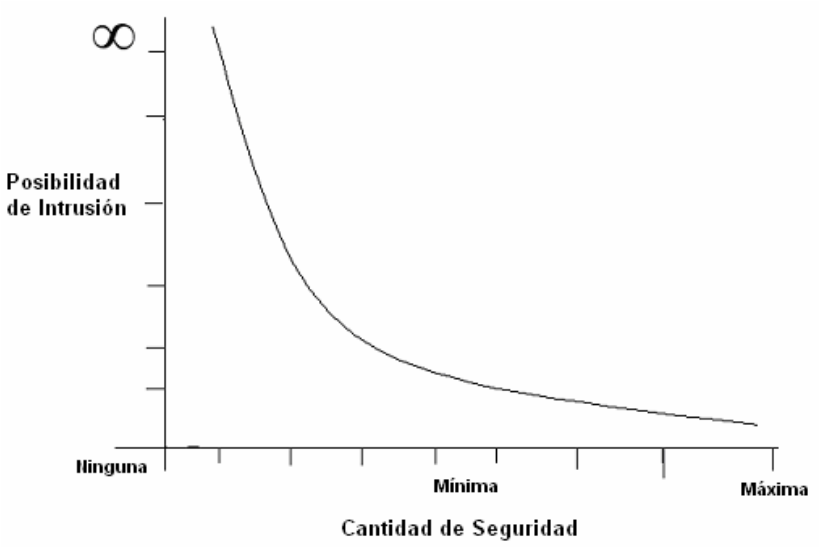


Figura 2.3 – Seguridad contra intrusión

Por consiguiente se debe buscar un equilibrio entre ambos aspectos con base en los requerimientos de la organización y de sus miembros, es decir, es necesario encontrar un punto de equilibrio entre ambos aspectos (figura 2.4).

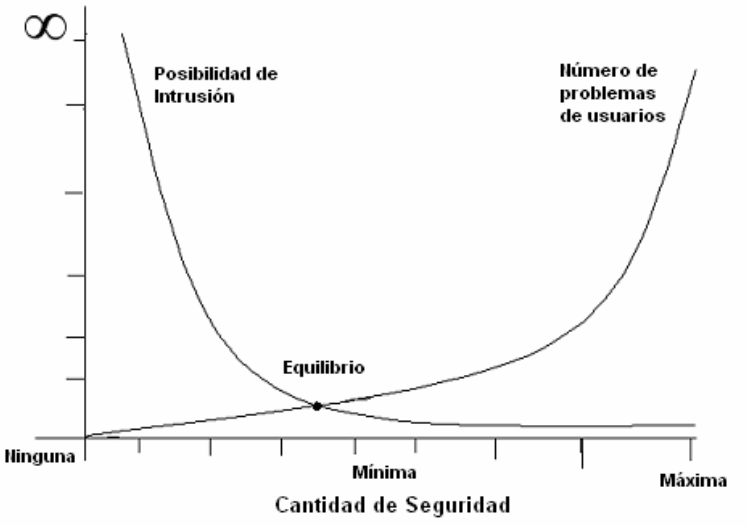


Figura 2.4 – Punto de equilibrio

El punto de equilibrio encontrado es un indicador de cómo deben ser balanceadas las medidas de seguridad informática enfocadas a prevenir en cierto grado intrusiones a los sistemas, con las restricciones impuestas al personal, las cuales

pueden representar ciertas molestias en el desempeño de las actividades normales de los usuarios.

2.2.1.- Criterios Para Establecer Políticas de Seguridad

En primera instancia, se debe recordar que al momento de establecer una política de seguridad es necesario basarnos en tres cuestiones básicas: qué es lo que necesitamos proteger, de qué lo vamos a proteger y cómo lo vamos a proteger. Para dar respuesta a estas interrogantes es necesario determinar los activos que necesitan protección, hacer un análisis de las vulnerabilidades y amenazas del sistema, así como establecer las medidas que se tomarán para proteger los sistemas.

De igual forma es importante tomar en cuenta que las políticas deben ser acordes a la realidad de la empresa, tratando que la seguridad sea parte de la operatividad común de la organización y no como un agente extraño. Para tales fines, es imprescindible que las políticas de seguridad consideren los siguientes puntos:

- Cubrir todos los aspectos relacionados con el sistema y abarcar todos los niveles del mismo, es decir, la parte física, la humana, la lógica y logística.
- Tomar en cuenta las interacciones entre las herramientas del sistema y el personal que hace uso de las mismas.
- El ambiente donde se desarrolla la organización debe ser considerado, las políticas deben adaptarse de acuerdo al entorno donde se pondrán en práctica, por ejemplo si se trata de una escuela, una institución bancaria, etcétera.
- Evaluar los riesgos, el valor del sistema protegido, así como considerar el uso que se le da al mismo.
- Debe adaptarse a un modelo restrictivo o permisivo.

La figura 2.5 muestra un esquema para el análisis de seguridad informática, donde se observan los diversos factores involucrados dentro del entorno de la protección a los sistemas:

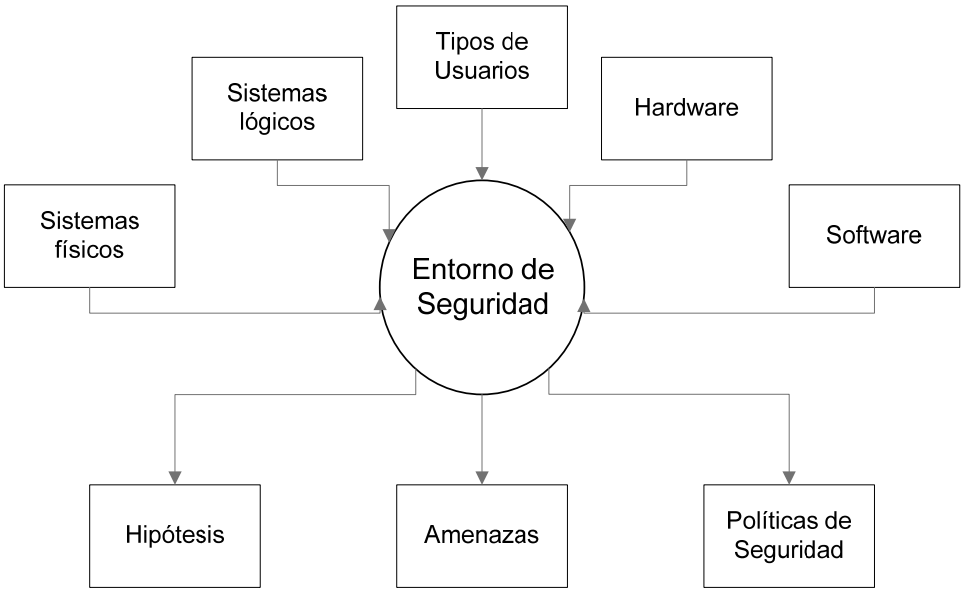


Figura 2.5 – Esquema de seguridad informática

El estudio del entorno de seguridad es la primera parte del análisis necesario para establecer un perfil de protección en el cual se encuentra el objeto de evaluación, mismo en el que se basaran las políticas de seguridad que se desarrollarán posteriormente.

2.2.2.- Modelos de Seguridad

Los modelos de seguridad son presentaciones formales de las diversas políticas de seguridad referidas a un sistema. El modelo debe representar las reglas que regulan la manera en que se debe manejar, proteger y como se debe distribuir la información delicada. Los modelos pueden ser de dos tipos: abstractos, si se ocupa de sujetos y objetos, o concretos, si traducen las entidades abstractas a entidades a un sistema real, como archivos o procesos.

"Los modelos sirven a tres propósitos en la seguridad informática:

- Promover un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas.
- Proveer una representación de una política general de seguridad de manera formal y clara.
- Expresar la política exigida por un sistema de cómputo específico."[7]

Los modelos a su vez, se dividen en:

- Modelos de control de acceso – Identifican las reglas necesarias para que un sistema sea asegurando en todos los accesos a sus recursos.
- Modelos de flujo de información – Se enfocan en el intercambio de datos, en la transferencia de la información.
- Modelo de integridad – Referente a que la información resulte consistente y el sistema pueda se ejecute correctamente.

Una matriz de acceso es un modelo de control que se utiliza principalmente para asegurar la confidencialidad y la integridad de los activos. Para éste caso la matriz no debe ser estática, es decir, deben existir cambios constantes, con la finalidad de que sea posible alterar sujetos y objetos, adaptándose a las condiciones que se presenten a lo largo de la vida útil del sistema.

Supongamos que en primera instancia se encuentran los usuarios de mayor rango, como pueden ser ejecutivos, gerentes, jefes de organizaciones o empresas. A continuación se encuentra el administrador de la red, quien debe poder tener acceso a la totalidad de los servicios ya que son su responsabilidad y es necesario que pueda acceder a ellos en caso de que exista una contrariedad.

[7] LÖPEZ Barrientos María Jaquelina, QUEZADA Reyes Cintia, "Fundamentos de Seguridad Informática" Universidad Nacional Autónoma de México, México, p.134

Posteriormente se encuentran los usuarios con privilegios, que pueden ser analistas financieros y de negocios, ingenieros, personal docente o investigadores. Finalmente contamos con usuarios comunes, quienes tienen un uso más limitado de los servicios de red. Entre ellos se encuentran personal de oficina y administrativos.

Se distinguen entonces entre tres tipos básicos de permisos disponibles para los diferentes tipos de usuarios, los cuales son:

- Lectura (R) – El servicio puede ser visto por el usuario pero no puede ser ejecutado y mucho menos modificado.
- Escritura (W) – El servicio puede sufrir alteraciones directas por parte del usuario, ya sea tanto en la creación como en la modificación de elementos dentro del mismo.
- Ejecución (X) – El servicio puede ser usado por el usuario, siempre y cuando esté no sufra alteración.

Por lo tanto, en forma de ejemplo general, se puede establecer una relación entre los usuarios y los servicios disponibles de la red como se muestra en la tabla de la figura 2.6, en donde los permisos otorgados dependen del tipo de usuario.

	Usuarios de mayor rango	**Administrador de la red**	**Usuarios con privilegios**	**Usuarios comunes**
Web	R, W, X	R, W, X	R. W, X	R, X
Archivos comparttidos	R, W, X	R, W, X	R, X	R
Correo electrónico	R, X	R, W, X	R, X	R, X
Firewall	R, X	R, W, X	X	X
IRC	R, W, X	R, W, X	R, X	-
FTP	R, W, X	R, W, X	R, W, X	R, X
SSH	R, W, X	R, W, X	R, X	-
Bases de Datos	R, W, X	R. W. X	R, W, X	R, X

Figura 2.6 – Matriz de control de accesos que muestra la relación entre servicios de red y tipos de usuario

2.3.- Consideraciones Sobre las Políticas de Seguridad

Como se ha mencionado, el principal problema para la creación de las políticas de seguridad se encuentra en la renuencia de los dirigentes de las organizaciones para establecer controles de seguridad, en gran parte por que el beneficio no resulta fácilmente perceptible.

Si bien, usualmente las organizaciones consideran que el establecimiento de reglas que permitan mantener resguardada la información de intrusos resulta intrascendental para su desarrollo y crecimiento, es necesario hacer ver que a la larga evitan pérdidas tanto económicas como de prestigio para la empresa, las cuales tienen grandes repercusiones a futuro.

La primera reacción más común para todo dueño de un negocio ante el planteamiento de una reestructuración de sus mecanismos de seguridad, es que la inversión destinada para estos fines resulta un desperdicio de recursos. Por lo

tanto, se debe dar una explicación en términos de balance entre el costo y los beneficios posibles.

Por consiguiente se vuelve necesario brindar diversas alternativas que amplíen el panorama de los miembros de la organización en cuestión, principalmente resulta de vital importancia conocer la perspectiva de los usuarios finales ya que serán ellos quienes tendrán contacto directo con la información.

Es importante entonces considerar que al definir las políticas informáticas se tomen en cuenta los siguientes puntos:

- Realizar un estudio para identificar y seleccionar lo que se debe proteger de acuerdo a la realidad de la empresa.
- Establecer niveles de prioridad e importancia sobre la información.
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos, imagen, credibilidad y productividad, la pérdida de datos sensibles.
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red.
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla.
- Crear conciencia en el personal sobre la importancia que tiene la seguridad de la información.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo beneficios y riesgos que se conllevaran.
- Realizar monitoreos periódicos con el fin de implementar respuesta a incidentes inesperados y lograr una recuperación inmediata con el fin de disminuir el impacto al mínimo.

Las políticas de seguridad deben especificar qué propiedades de seguridad debe proveer el sistema, del mismo modo que debe definir la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de cada una de las personas, con base en esto

podremos entonces asegurar que un sistema es seguro si cumple con las políticas de seguridad impuestas por la organización.

Es importante hacer notar que el personal dedicado a la seguridad no necesariamente son los encargados de realizar la valoración de riesgos, por lo que es importante distinguir entre las diversas responsabilidades a fin de garantizar que los diferentes procesos de valoración sean realizados por una persona especializada en el área.

Finalmente, es necesario integrar las políticas de seguridad a las estrategias del negocio, a su misión y su visión, con el propósito que aquellos que toman las decisiones hayan participado tanto en el proceso de valoración de riesgos como en la identificación de políticas de seguridad con la finalidad de que reconozcan la importancia que radica en ellas y su incidencia en las utilidades de la compañía.

Capítulo 3

Intrusiones a los Sistemas Informáticos

Capítulo 3
Intrusiones a los Sistemas Informáticos

No hay sistema alguno que sea totalmente seguro, siempre existirán fallas inherentes o externas que permitan vulnerar la integridad de los sistemas de información. Es por ello que se vuelve importante conocer las principales amenazas que actualmente existen a fin de establecer métodos para poder contrarrestar dichos peligros.

Las principales causas de explotación de fallas y de intentos de ataques en contra de la seguridad varían en gran medida, puede ser en algunos casos como parte de una experimentación, una especie de reto personal, mientras que en otros puede buscarse un beneficio personal ajeno a los intereses de la empresa. Por consiguiente existe una gran gama en la manera en que pueden realizarse las intrusiones, pero pueden establecerse mecanismos primordiales en la manera en que esto sucede:

- Ataques derivados de programas y sistemas mal configurados debido a descuidos o desconocimiento de los usuarios.
- Ataques a los sistemas y programas con vulnerabilidades conocidas, es decir, errores de programación presentes en el software, siendo esto último el más recurrente.

Así mismo las consecuencias derivadas de ataques a los sistemas son también de naturaleza variada. Los diversos tipos de ataques pueden desde ocasionar simples alertas o retrasar ligeramente las actividades de los usuarios hasta generar pérdidas económicas, de credibilidad o incluso de prestigio en empresas e instituciones.

Solamente cuando conozcamos los alcances y la manera de actuar de las diferentes amenazas, podremos establecer los mecanismos de seguridad necesarios para cada uno de los diferentes elementos que conforman los sistemas de comunicaciones, así como la mejor manera de contrarrestar los diversos esquemas de ataques existentes.

3.1.- Principales Vulnerabilidades y Tipos de Intrusiones

Resulta bastante complejo establecer una métrica para medir el alcance de las intrusiones a los sistemas informáticos. De acuerdo a la CERT (Computer Emergency Response Team), las estadísticas más recientes con las que cuenta en relación al número de vulnerabilidades reportadas y de los incidentes registrados en los Estados Unidos son los siguientes:

- "Vulnerabilidades Reportadas (2006) 8'064
- Reportes de Incidentes (2003) 37'529

Debido al uso de herramientas de ataque automatizadas, los ataques en contra de los sistemas conectados a Internet han tomado un lugar tan común, que el conteo de número de reportes de incidentes provee poca información referente a los alcances y el impacto de los ataques."[8]

[8] Fuente: CERT/CC

Por consiguiente resulta conveniente conocer de manera general los diferentes tipos de amenazas y la manera en que éstas operan, así como el grado de riesgo que representan, a fin de poder establecer medidas realistas de prevención y corrección que permitan neutralizarlas.

La mayoría de los casos en que los sistemas resultan comprometidos es por causas de origen interno a la organización, así como por carencia de políticas que obliguen a los usuarios a tomar las medidas de precaución pertinentes. Por tal motivo, el administrador de los sistemas informáticos debe conocer a fondo las amenazas existentes ya que primero es necesario conocer lo que se debe defender y de qué se va a proteger.

3.1.1.- Spyware

Se conoce como spyware a aquellas aplicaciones que buscan obtener algún tipo de información sin el consentimiento del usuario. Regularmente estas aplicaciones, pertenecientes a la gama de software conocido como malware, se instalan al descargar contenido ilícito de Internet, o bien, cuando se da clic en anuncios publicitarios que no resultan sospechosos en primera instancia, como por ejemplo, en el caso de los pop-ups.

Existe una gran variedad de técnicas que pueden ser implementadas para la recolección y el envío de información vía e-mail, entre las más recurrentes se encuentran el uso de keyloggers, es decir, herramientas que permiten guardar un registro de toda la información ingresada a través del teclado, la realización de copias del historial de navegación en red o bien el escaneo de archivos en el disco duro.

Los objetivos que se persiguen con este tipo de aplicaciones son muy diversos, desde recolectar información de sitios visitados para posteriormente venderlos a

alguna agencia publicitaria, hasta la de obtener números confidenciales y contraseñas de cualquier índole con fines ilícitos.

A diferencia de los virus y los gusanos informáticos, el spyware usualmente no se auto-replica para infectar a otros equipos, en realidad puede considerarse como una herramienta de administración remota, ya que en algunos casos el atacante no sólo envía y recibe información, sino que también puede ganar el control de otras aplicaciones. Un ejemplo son los dialers, aplicaciones que alteran el acceso telefónico a Internet con el fin de imputar cargos monetarios al usuario que haga uso del equipo en cuestión.

Actualmente mucho del spyware está diseñado para atacar vía Internet Explorer, debido principalmente a la profunda integración de esta aplicación con el sistema operativo Windows. La mayoría de los casos sucede mediante la instalación de "extensiones de ayuda" para el navegador, los cuales modifican el comportamiento del sistema y redireccionan el tráfico.

Es necesario hacer notar que no necesariamente todo el spyware que encontremos en línea es resultado de actos intencionales. En muchos casos, los sitios pueden ofrecer programas infectados sin que el administrador sea consciente de ello. Por esto mismo es necesario que quien cuenta con un sitio en línea verifique que no sea afectado por los siguientes aspectos:

- "Malware disponible para descargar desde el sitio.
- Malware disponible en sitios a los que se enlaza.
- Malware distribuido a través de anuncios presentes en el sitio.
- Malware en enlaces generados por los visitantes.
- Ataques hackers al sitio."[9]

[9] Fuente: Stopbadware.org

Es entonces que se hace necesario contar con la colaboración de varios sectores para poder disminuir la amenaza que representa el spyware, ya que como se ha visto representa un serio riesgo a la integridad de los sistemas. En resumen los principales riesgos por una falta de atención a este tipo de intrusiones son los siguientes:

- Atentados contra la privacidad del usuario o la organización.
- Reducción en el rendimiento de los sistemas.
- Malfuncionamiento de aplicaciones.
- Costos económicos.

3.1.2.- Spoofing

El spoofing es una técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falsificada. Desde su equipo, el atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema, el cual ha establecido algún mecanismo de confianza basado en el nombre o la dirección IP del host suplantado.

Este tipo de ataque resulta más efectivo donde existen relaciones de confianza entre las máquinas de una red, por ejemplo, en algunas corporaciones es común tener configuraciones en donde no es necesario registrar un usuario y contraseña para ingresar a las máquinas.

Principalmente se utilizan ataques de denegación de servicios, es decir enviando enormes cantidades de paquetes que sobrecargan el tráfico de la red, sin la necesidad de preocuparse de recibir las respuestas de la víctima. Aunque actualmente se hace un mayor uso de bots, es decir, programas autómatas que realizan funciones de explotación de ciertas vulnerabilidades, el spoofing sigue constituyendo una amenaza latente que es necesario considerar al establecer mecanismos de protección.

Los principales ataques de falseamiento de identidades se dividen en los siguientes grupos:

- DNS Spoofing – Falsificación de una dirección IP, resolviendo con un nombre falso dicha dirección IP.
- ARP Spoofing – Solicitud y respuestas ARP falseadas a fin de que un equipo dentro de una red local envié los paquetes a una máquina atacante en lugar de hacerlo a su destino legítimo.
- Web Spoofing – Visualización y alteración de una página Web.
- E-mail Spoofing – Falsificación de la cabecera de un correo electrónico a fin de que el remitente parezca legítimo.

3.1.3.- Denegación de Servicios

Este tipo de ataque (conocido también como DoS por sus siglas en inglés) tiene como finalidad hacer inaccesibles los recursos computacionales a los usuarios legítimos. Usualmente es empleado en ataques a servidores, haciendo que los servicios Web dejen de estar disponibles temporalmente.

Hay dos maneras principalmente de ejecutar un ataque de denegación de servicios, forzando a las máquinas víctimas a consumir una gran cantidad de recursos a fin de que no se puedan proveer los servicios para los que originalmente están diseñadas, o bien obstruir la comunicación entre el cliente y servidor de tal manera que no pueda existir conexión entre ambas partes.

“Ya que no todas las interrupciones y fallas en las redes pueden ser ataques DoS, es necesario identificar los patrones que muestran este tipo de intrusiones:

- Comportamiento de conexión inusualmente lenta (al abrir archivos o al acceder a sitios Web).

- Indisponibilidad de un sitio Web en particular.
- Imposibilidad de acceder a cualquier sitio Web.
- Incremento dramático en la cantidad de spam que se recibe en una cuenta."[10]

Uno de los métodos más comunes para la ejecución de este tipo e ataques es el conocido tipo flood (inundación), en el cual el objetivo es saturar a la víctima con peticiones de respuesta de conexión. Hay diversas variantes de este tipo de ataques, pero trabajan de manera similar.

Un claro ejemplo, es el caso particular de un ataque smurf, que es una variación de un flood ICMP. En este caso, se envía un paquete a una dirección de difusión, cuyo objetivo original es enviar un mismo paquete a diversos destinos dentro de una red IP, por ejemplo para la red 192.168.0.0, la dirección de difusión será la192.168.255.255.

El ataque consistiría en enviar paquetes ICMP a esta dirección de difusión, lo cual provocaría una severa saturación en la red al existir una enorme cantidad de computadoras que intentan establecer respuestas. En la figura 3.1 se muestra la naturaleza de este ataque:

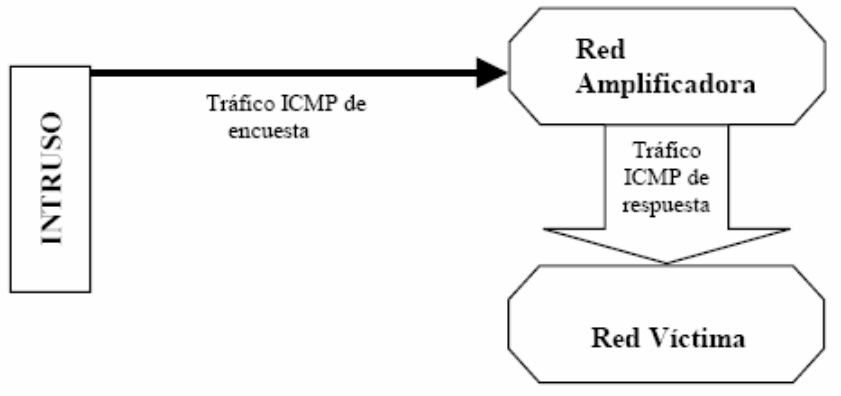


Figura 3.1 – Representación de las partes de una ataque smurf

[10] Fuente: US-CERT

La mejor herramienta para combatir este tipo de problemas es la prevención, ya que una vez iniciado el ataque, remediarlo tiene un gran costo, tanto en el aspecto económico como en el factor tiempo, por lo que en la planificación de los servicios es importante considerar estos aspectos.

El uso de routers y switches puede ser una gran ayuda, ya que estos dispositivos actualmente cuentan con listas de control de accesos que evitan ataques como el descrito anteriormente. Una de las mejores soluciones es la implementación de un firewall correctamente configurado que brinde robustez en su funcionamiento, es decir, que además de evitar el acceso a la salida de paquetes por ciertas direcciones IP, también establezca un límite de peticiones y respuestas.

3.1.4.- Spam

El spam es el envío de mensajes de manera masiva a diversos destinatarios, cuyo contenido es en su gran mayoría de tipo publicitario, y los cuales resultan indeseados para los usuarios. Generalmente el término se utiliza de manera indistinta para referirse al correo basura, pero también es aplicable en otras áreas, como mensajes spam en blogs, foros, celulares o motores de búsqueda.

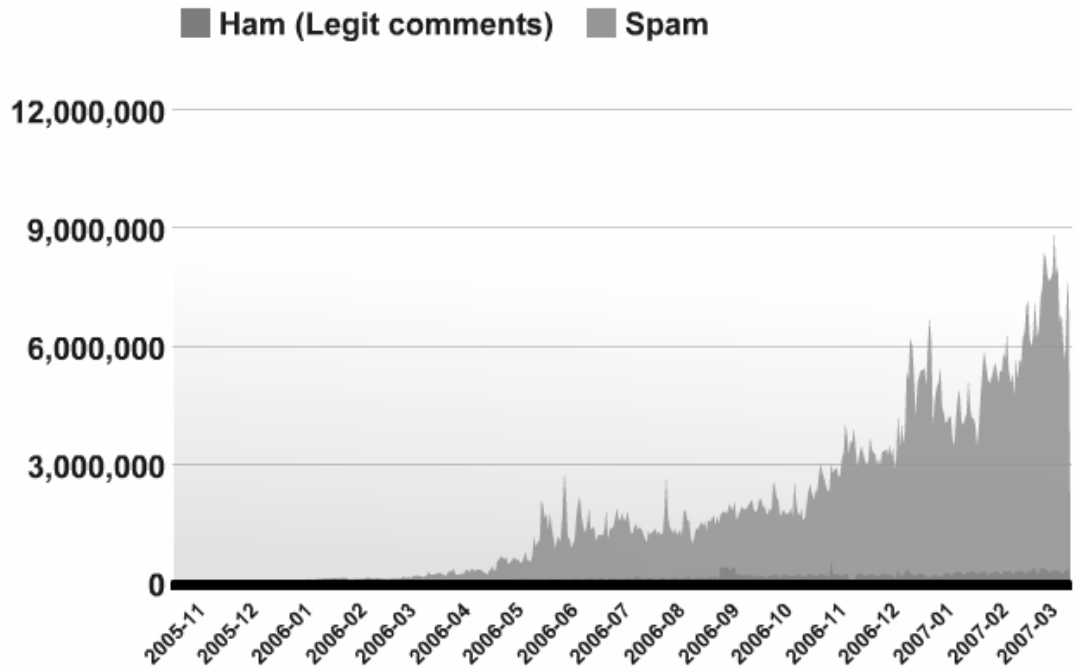
Si bien, el principal objetivo de los mensajes spam es promocionar algún servicio o producto a un muy bajo costo, existen otras vertientes bastante difundidas, como es en el caso de promover ideas religiosas o políticas. En algunos casos no se busca ningún fin en particular, más que el de probar nuevas vulnerabilidades en los servidores de correo.

La manera en que opera el correo spam es en primera instancia conseguir o generar una base de datos con una lista de correos electrónicos a los cuales enviar los mensajes, posteriormente se utiliza un programa que recorre la lista de direcciones válidas obtenida, y finalmente se espera la verificación de que los mensajes hayan sido recibidos, lo cual se puede lograr mediante diversos

métodos, por ejemplo, incluir una imagen que se descargue desde un servidor perteneciente a quien envió los correos.

También se da la posibilidad de enviar correos spam con algún tipo de malware, el cual infecte al equipo de la víctima a fin de que ésta se vuelva un emisor de correos spam y crear entonces lo que se conoce como una computadora zombi. El atacante puede entonces utilizar a su voluntad la lista de contactos con la que cuente la máquina perpetrada con el fin de repetir este ciclo de manera indefinida.

El problema se ha vuelto bastante complicado ya que la gran mayoría de los mensajes enviados resultan ser spam. En la gráfica de la figura 3.2 se puede apreciar la estadística registrada por la compañía Askimet en lo referente a mensajes legítimos en los blogs contra los mensajes spam:



"Total spam:913,925,834

Total ham:50,499,812"[11]

Figura 3.2 – Mensajes spam contra mensajes legítimos (ham)

[11] Fuente: Akismet (14-marzo-2007)

El spam afecta directamente a los recursos empleados en las redes, así como la producción por el tiempo invertido por las personas en revisar este tipo de mensajes. También existen costos y daños indirectos, cuando se trata de algún fraude financiero, robos de identidad o bien, cuando los mensajes spam llevan contenido ofensivo para las personas

Hay varias estrategias que se pueden seguir para evitar el spam, o en todo caso, disminuir la cantidad de mensajes basura en el correo. Algunas de las medidas más comunes son no reenviar mensajes que sean parte de una cadena de correo, limpiar las direcciones de correo cuando se reenvía un mensaje, escribir la dirección de manera modificada a fin de evitar el rastreo automático por parte de bots, por ejemplo sustituir la letra @ por (arroba) en direcciones de correo, lo cual representa una alteración bastante considerable en el algoritmo necesario para rastrear direcciones de correo electrónico.

3.1.5.- Inyección de Código SQL

Una de las vulnerabilidades más conocidas en las bases de datos es la inyección de código SQL. El atacante aprovecha errores y fallas en los filtros de los campos para ingreso de datos de los sistemas, colocando en esa parte código que puede ser interpretado por el servidor.

Structured Query Language (SQL) es el lenguaje más popular para crear, mantener, actualizar y eliminar información de una base de datos. Si bien existen diversas variantes del mismo, la mayoría utiliza las mismas palabras clave para realizar las principales acciones, por lo que los atacantes pueden seguir ciertos patrones al momento de intentar comprometer un sistema.

El modo en que opera este tipo de ataques se ilustra con el siguiente ejemplo. Se tiene la siguiente línea de código para hacer una consulta de la tabla “usuarios” en

una base de datos y “nombre_ingresado” es la variable que se recibe desde el campo correspondiente del formulario en el sistema:

*“SELECT * FROM usuarios WHERE nombre = ‘” + nombre_ingresado + “’ ; “*

Originalmente en la sentencia, debería buscarse a todos los usuarios que cumplan con la regla de que sean iguales a la variable ingresada. Sin embargo si se coloca lo siguiente en el campo de “nombre_ingresado”:

’ OR ‘1=1

El resultado que se tiene al sustituir el valor de la variable es:

*“SELECT * FROM usuarios WHERE nombre = ‘’ OR ‘1=1’ ; “*

lo cual es una sentencia cierta ya que para este caso particular se genera una sentencia verdadera forzada, y ésta permitiría un ingreso válido a la base de datos sin la necesidad de validar al usuario.

Existen acciones más peligrosas como eliminar tablas, crear usuarios con privilegios de administrador, todo depende de la habilidad del atacante y de sus conocimientos en bases de datos, por lo que el impacto de este tipo de intrusiones puede resultar muy alto.

Para solucionar este tipo de problemas se deben tomar diversas medidas. La primera como se mencionó es establecer filtros que permitan validar que el usuario está ingresando los datos que se esperan, es decir, que no existan espacios en blanco o bien que se agreguen diagonales extras cuando se detecte algún tipo de símbolo extraño. También, si es posible, validar el tipo de dato que se está manejando, por ejemplo, verificar que los datos de identificación sean sólo de carácter numérico, todo esto a fin de reducir los riesgos.

Algunas medidas adicionales son asegurarse de nunca dar permisos de administrador a más de un usuario, así como establecer una jerarquía de permisos bastante sólida a fin de que no se pueda escalar a través de estos. También se recomienda utilizar el cifrado de la información a fin de que los datos recibidos en la base de datos no se almacenen en claro.

3.1.6.- Rootkits

Un rootkit es una colección de herramientas de software cuyo principal propósito es lograr acceso a los recursos de un sistema, usualmente con fines maliciosos, aunque en otros casos puede ser empleado para auditoría de redes y sistemas al probar la fortaleza y seguridad de estos mismos.

Los rootkits usualmente hacen uso de backdoors para ocultar las aplicaciones que permiten el acceso al sistema mientras se realiza un ataque. También es posible que sean usados para que una vez que se ha ganado el control de una computadora, usarla para realizar ataques a otros equipos.

Existen cuatro tipos de rootkits:

- Virtualizados – Trabajan en el nivel más bajo, modificando la secuencia de inicio del sistema operativo para iniciarse a sí mismos. Una vez en el sistema, este tipo de rootkit intercepta toda comunicación entre el hardware y el sistema operativo.
- Nivel de de kernel – Reemplaza algunas líneas originales del kernel para insertar backdoors en el sistema operativo de la computadora. Este tipo de rootkits crean inestabilidad en el sistema perpetrado y resultan muy difíciles de detectar.
- Nivel de librería – Usualmente reemplaza o parchan llamadas al sistema operativo con versiones que ocultan información del atacante.

- Nivel de aplicación – Reemplazan archivos binarios originales con troyanos.

Lograr remover con éxito un rootkit es bastante complicado por lo que en la mayoría de los casos resulta más conveniente reinstalar el sistema operativo en su totalidad.

3.2.- Errores Prevenibles en los Sistemas Informáticos

A fin de reforzar los sistemas de control de incidentes, es necesario establecer buenas prácticas de control y configuración que aseguren que tanto la tecnología empleada, como la gente que hace uso de los equipos de cómputo no sean motivo de problemas en la infraestructura de los sistemas. Asimismo, dichas prácticas deben ofrecer garantías en cuanto a que los riesgos de intrusión o daños a la información sean los mínimos posibles.

Una mala configuración o un descuido en la estructura de la seguridad pueden acarrear graves consecuencias. Generalmente la mayoría de las medidas de seguridad se enfocan en posibles descuidos de los usuarios, así como de posibles intrusiones externas por medio de ataques a la organización. Sin embargo, es necesario considerar varios aspectos más cercanos a los administradores.

En muchos de los casos, se debe prevenir cualquier tipo de acción por sencilla que parezca, o bien, que resulte en apariencia tan obvio que pueda llegar a pasar desapercibida. Por consiguiente, ninguna medida de seguridad resulta excesiva ni tampoco intrascendente, aunque esto pudiera parecer algo paranoico.

Si bien la tecnología puede brindarnos cierta confianza en su eficacia, el factor humano juega el papel más importante, ya que las personas son finalmente quienes administran los sistemas y dependerá de su capacidad hacer que las herramientas con que se cuentan funcionen de la mejor manera posible.

Muchos descuidos ocurren por una falta de análisis en los detalles finales, así como por suponer que si un sistema se encuentra funcionando correctamente en su inicio, seguirá así por el resto de su vida útil. Sin embargo, existen diversas fallas que pueden ser aprovechadas incluso sin la necesidad de tener profundos conocimientos en computación.

Finalmente son los detalles los que determinan la calidad de un buen servicio, por lo que en seguridad informática ésta no es una excepción. Es necesario tener en mente que cualquier fallo mínimo puede tener costos bastante elevados, por lo que las políticas que se tengan para regular las actividades de una organización deben de considerar este tipo de situaciones.

3.2.1.- Manejo de Contraseñas

Las contraseñas son claves de acceso a recursos de cierta importancia, por lo que es necesario tener establecidas reglas con los requisitos que deben cubrir dichas claves y el control que debe existir sobre las mismas. Existe una gran cantidad de casos de descuidos en este último rubro, ya que debido a que no resulta ser algo tangible, no se tiene la noción de la importancia que encierra una clave.

Los algoritmos utilizados para guardar las contraseñas son bastante robustos en la actualidad, por lo que descifrar una clave resulta bastante difícil para un atacante si es que se han establecido ciertas normas que aseguren la fortaleza en las contraseñas. Para tal fin se deben establecer las políticas de seguridad correspondientes en esta área, siendo lo más importante que toda las personas que laboran en el lugar las conozcan y las pongan en práctica.

Desafortunadamente, la mayoría de las personas utilizan palabras sencillas o relacionadas a su ámbito personal, por lo que es posible que un intruso pueda prescindir de herramientas tecnológicas y sencillamente adivinar la clave probando

una serie de palabras relacionadas con el usuario, o bien hacer uso de la ingeniería social para obtener ciertos datos personales que puedan ser usados como fechas, números de la suerte o nombres.

Para evitar este tipo de situaciones se recomienda que el sistema sólo tenga un número limitado de intentos para escribir la contraseña así como, dependiendo si la información resulta realmente sensible, exista un tiempo límite para autenticarse y sobre todo establecer un tiempo de vida de las claves, esto es que exista una política de cambio de contraseñas.

Algunos otros aspectos que se deben cuidar es que no se dejen las contraseñas en lugares visibles para cualquier persona o en lugares de fácil acceso, como puede ser abajo del teclado. También debe tenerse especial cuidado al momento de eliminar un papel con este tipo de información, ya que una persona malintencionada puede buscar información en la basura, una práctica conocida como trashing.

Es importante recalcar el aspecto crítico que representa una contraseña, por lo que dependiendo de la importancia de los recursos y lo expuestos que pudieran estar, se deben tomar medidas extras de protección, como por ejemplo, para el caso de servidores se recomienda no tener conectado un teclado a éste, y evitar la entrada de personal que no esté autorizado.

Por otra parte las contraseñas deben ser sencillas en su manejo, por lo que deben ser fáciles de recordar, a fin de evitar la necesidad de tener algún recordatorio de la misma. También debe evitarse difundir o dar a conocer la contraseña a varias personas, ésta debe ser de uso privado y confidencial, y deben existir mecanismos que regulen el período de vida de las mismas.

3.2.2.- Exploits

Los exploits son programas maliciosos, fragmentos de código o una secuencia de comandos que buscan aprovechar o tomar ventaja de algún error o vulnerabilidad en el software a fin de ocasionar cierto comportamiento inesperado en el sistema con el objetivo de lograr ganar control en el mismo.

Este tipo de fallas en los sistemas son encontradas de diversas maneras, ya sea después de realizar pruebas y detectar posibles errores, de manera accidental por parte de algún usuario legítimo, o bien por un atacante a fin de poder ganar acceso de manera ilícita, lo cual convierte a los exploits en una amenaza de muy alto riesgo ya que no existe una solución inmediata disponible.

Hay varios criterios usados para clasificar a los diversos tipos de exploits existentes. La manera más común de agruparlos es por la forma en cómo el exploit entra en contacto con el software vulnerable, siendo las siguientes:

- Exploit remoto – Es aquel que funciona a través de una conexión en red, y no es necesario que el atacante haya tenido ingresar directamente al sistema vulnerable.
- Exploit local – El atacante necesita forzosamente haber ingresado al sistema y contar con ciertos privilegios de administrador para poder comprometer al equipo.

Otra clasificación se deriva del tipo de daño ejercido en contra de los sistemas, como son la denegación de servicios, la ejecución de código, el desbordamiento de buffer o el acceso no autorizado a datos, pero debido a la gran diversidad y variedad de vulnerabilidades posibles, resulta complicado tener una clasificación precisa basada en este criterio.

Debido a la naturaleza inherente de los exploits, no existe una manera segura de prevenir el ataque hasta que se da a conocer la falla y se ha obtenido una manera de cómo corregir el problema por medio de un parche. Sólo hasta el momento en que se publica la vulnerabilidad y la manera en que puede ser corregida, el exploit correspondiente se vuelve obsoleto y deja de ser una amenaza.

Es por ello que resulta conveniente mantenerse informado sobre los nuevos descubrimientos en el área de seguridad para conocer las amenazas que surgen todos los días, así como mantener actualizado el software de los sistemas en la versión más estable disponible a fin de corregir diversos errores de programación y vulnerabilidades que ponen en riesgo la información.

3.2.3.- Servicios Activos Innecesarios en los Sistemas

Uno de los principales errores por parte de los administradores de las redes es la falta de prevención al momento de instalar un sistema. Es importante revisar que no existan servicios como ftp, telnet o ssh si éstos o cualquier otro no son necesarios ya que hay diversos casos de intrusión por el descuido de dejar puertos habilitados, siendo que en todo caso pudo ser esto prevenido.

Ya que existen herramientas que escanean los diversos puertos disponibles de manera automática, es bastante viable que un programa intruso pueda ingresar a través de un puerto que se encuentre abierto y sin ningún tipo de protección. También existe el caso de que alguien pueda identificar el sistema operativo en cuestión e intente probar diversas formas de acceso que se encuentren habilitadas por defecto.

La mayoría del software viene con algún tipo de programa de autoinstalación, y cuyo objetivo es facilitar la instalación de dichos paquetes, dejando la mayor parte de las funciones disponibles y habilitadas. La filosofía que se sigue por parte de la mayoría de los fabricantes es instalar la mayoría de los componentes y habilitar

sus funciones en lugar de dejar que el usuario vaya instalando funciones adicionales conforme sea necesario.

Este tipo de situaciones generan muchas vulnerabilidades que no resultan visibles en primera instancia, ya que como se mencionó, la mayoría de los usuarios no son conscientes de lo que están instalando, y dejan expuesto al sistema con rutas libres para un atacante. En el caso de diversos sistemas operativos, usualmente se dejan abiertos diversos puertos que pueden ser aprovechados con fines dañinos, por lo que debe hacerse lo posible por habilitar sólo aquellos que resulten necesarios a fin de disminuir las posibilidades de intrusión.

Aunque se cuente con un firewall, programas antispyware y antivirus, se deben tomar las precauciones mencionadas, ya que el software es perfectible y este tipo de intrusiones a diferencia de los exploits son completamente prevenibles con el seguimiento de simples reglas de seguridad.

"En la mayoría de los crímenes (informáticos), el 84 por ciento pudo haber sido prevenido si la identidad de las computadoras conectadas fueran revisadas aparte del usuario y password"[12]

3.3.- Datos Estadísticos de Ataques a las Redes

Un reciente estudio sobre crímenes informáticos realizado por la compañía norteamericana "Trusted Strategies" en comisión por "Phoenix Technologies", arroja diversos datos importantes relacionados principalmente a la conducta de los atacantes de los sistemas y el daño a los sistemas de seguridad.

[12] "Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006", pp.3

A través de estos datos podemos establecer ciertos patrones que nos permitan mejorar las medidas de seguridad, así como crear estrategias que eviten intrusiones que originalmente pudieron haber sido prevenidas.

Uno de los datos más sobresalientes es la ubicación del atacante. En la mayoría de los casos se realizo desde la casa del intruso, como se muestra en la gráfica de la figura 3.3, lo cual indica que existen graves problemas de protección, y los mecanismos que se utilizan actualmente para resguardar los recursos de las empresas son ineficientes.

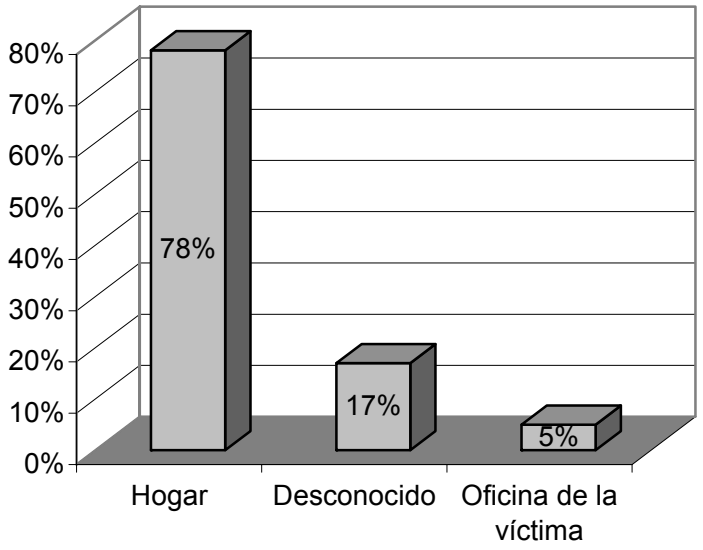


Figura 3.3 – Localización del atacante[13]

La mayor parte de los daños ha sido producto de un descuido en los mecanismos para manejar usuarios y contraseñas, siendo mucho mayores las pérdidas que las ocasionadas por virus, gusanos u otros métodos que no implican registrarse como usuario. En la gráfica de la figura 3.4, se muestra la estimación porcentual de ataques que pudieron ser prevenidos si se contara con un mecanismo de identificación más complejo.

[13] Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006", pp.3

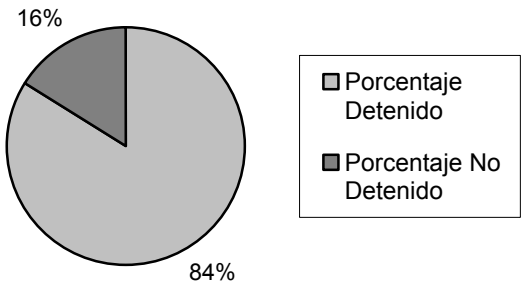


Figura 3.4 – Porcentajes de mecanismos de identificación que pudieron prevenir ataques.[14]

Sin embargo la mayoría de la inversión tanto económica como de tiempo se destina a medidas de seguridad contra virus e intrusiones por parte de gente externa a la empresa, cuando la realidad nos dicta que muchos de los problemas tienen raíz en el interior de las organizaciones.

Muchos de estos problemas pudieron prevenirse si existiera la conciencia de la necesidad de establecer controles mínimos. Si las contraseñas se renovaran constantemente y los dispositivos para la validación de los usuarios fueran más elaborados, la gran mayoría de las intrusiones ocurridas pudieron haberse evitado.

Como se puede apreciar en la gráfica de la figura 3.5, casi la mitad de los ataques están relacionados de alguna manera con gente que trabaja dentro de las empresas, a quienes se le conoce también como “insiders”, lo que nos indica que una buena parte de los problemas pueden ser corregidos estableciendo controles más estrictos dentro del área de la informática para las personas que tengan algún tipo de contacto con la organización

[14] Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006”, pp.6

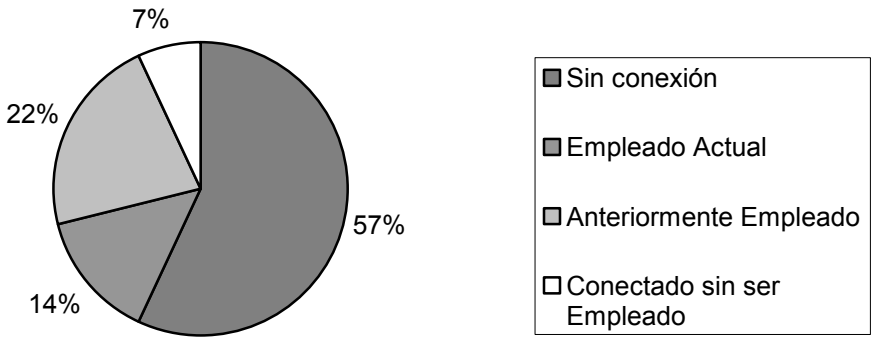


Figura 3.5 – Relación del atacante con la víctima[15]

Debido a que la gran parte de las intrusiones son por parte de gente interior a las empresas, podemos observar que no fue necesario hacer uso de profundos conocimientos de informática para poder perpetrar los equipos, en la mayoría de los casos se debió a que se pudo conseguir el usuario y la contraseña de los equipos que cuentan con información sensible para acceder a ellos desde el hogar de los perpetradores.

La mayoría de los ataques pudieron ser prevenidos, sin importar si se trataban de intrusiones externas o internas, si se establecieran mejores mecanismos para poder validar a los usuarios, ya que como se mencionó anteriormente, en la mayoría de las empresas el único medio que se utiliza para validar a los usuarios es una clave, la cual a su vez en su mayoría resulta ser bastante sencilla y fácil de obtener o adivinar.

[15] Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006", pp.7

Capítulo 4

Medidas de Seguridad

Capítulo 4
Medidas de Seguridad

Actualmente hay una gran cantidad y diversidad de amenazas existentes, por lo que han surgido varios mecanismos tecnológicos con los cuales hacerles frente. Debido a que los problemas resultan ser bastante variados, es imposible asegurar y proteger un sistema con el uso de una tecnología específica. Por consiguiente debe existir una combinación de medidas de seguridad a fin de poder proteger los diversos activos de las organizaciones.

Una vez que se conoce el tipo de amenazas a las que se están expuestos los activos, y la manera en que éstas operan, es necesario conocer las herramientas disponibles, así como el funcionamiento de las mismas para poder prevenir o tomar las medidas de acción pertinentes en contra de las intrusiones que pudieran presentarse.

Como se mencionó en capítulos anteriores, es necesario hacer uso de diversas tecnologías para protegerse de los distintos tipos de intrusión y es con base en las políticas establecidas que se debe hacer la selección de las herramientas que se utilizarán, así como la manera en que serán implementadas a fin de obtener el mayor equilibrio entre el costo y el beneficio.

Ya que las necesidades de cada organización son diferentes, los requerimientos de cada una también lo son. Por lo tanto es obligación de el administrador de los sistemas conocer las diferentes opciones en el mercado y los nuevos avances que se tienen cada día. Deben considerarse las diferentes posibilidades que se tienen

en el ramo de la seguridad a fin de poder establecer la mejor solución para la empresa y asegurar el óptimo funcionamiento en el área informática.

Como se ha visto, la mayor parte de los problemas en la seguridad tienen su origen en el factor humano, por consiguiente debe considerarse al momento de implementar alguna solución con respecto a la prevención o corrección de intrusiones, ya que finalmente serán las personas que laboran dentro de la organización hacer que las herramientas implementadas resulten efectivas.

4.1.- Firewall

Un firewall es un elemento de software o hardware utilizado para establecer un control de acceso a una red de computadoras, previniendo comunicaciones no permitidas por las políticas de seguridad. La principal idea es que el firewall actúe como un filtro permitiendo que sólo los paquetes autorizados, es decir aquellos que cumplan con ciertas reglas preestablecidas e indicadas mediante las políticas de seguridad de la organización, puedan pasar libremente a través de la red.

Se distinguen dos tipos de firewall de acuerdo al nivel que funcionan dentro del modelo OSI:

- En capa de red - Funciona como filtro de paquetes IP, impidiendo que estos pasen si no cumplen con las reglas establecidas por el administrador. En la figura 4.1 se muestra un diagrama general de la ubicación de un firewall de este tipo.
- En capa de aplicación - Trabaja todo el tráfico HTTP, y puede filtrar los paquetes que entran o salen desde las aplicaciones que corren en red.

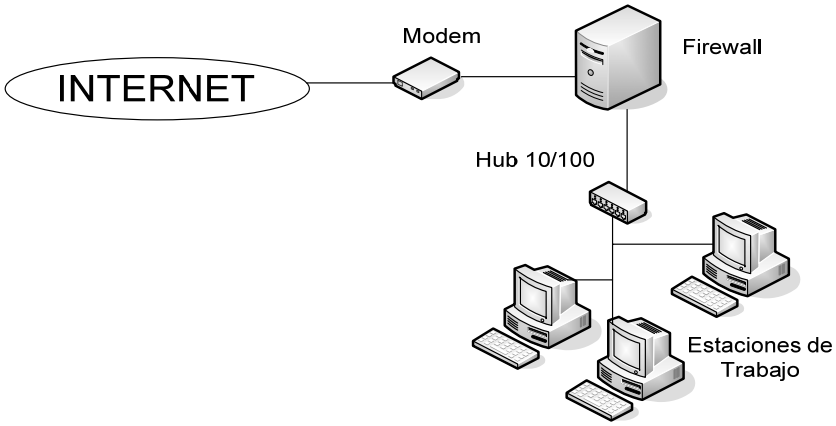


Figura 4.1 – Firewall en capa de red

La principal ventaja que se cuenta con un firewall que funciona en capa de red sobre uno de aplicación es que el control de flujo de información se centra en un sólo punto, por lo que si las reglas de filtrado han sido establecidas de manera correcta, no existe la necesidad de configurar cada uno de los equipos para que cumplan con dichos lineamientos, lo cual puede resultar un gran inconveniente cuando se cuenta con una gran cantidad de equipos conectados a la red.

Otro problema surge cuando se tiene una red inalámbrica, en la que cualquier persona con el equipo apropiado puede tener acceso dentro de la organización. En estos casos resultaría demasiado complicado establecer un control en los equipos si se utilizaran filtros a nivel de aplicación. Sin embargo, si se tienen un firewall que trabaje en capa de red, se pueden restringir los paquetes de información no deseados configurando sólo un equipo que esté dedicado a éste fin, el cual deberá ser ubicado en un área estratégica.

Para configurar correctamente un firewall es necesario contar con profundos conocimientos de los protocolos de red y de seguridad en cómputo. Cualquier descuido en estos aspectos puede originar vulnerabilidades que pueden ser aprovechadas por programas maliciosos o personas que busquen obtener un beneficio ilícito de la red.

Existen dos tipos de políticas que regulan el funcionamiento de cualquier tipo de firewall:

- Políticas permisivas – En éstas se permite el paso de los paquetes siempre y cuando no rompan con alguna regla establecida por el administrador.
- Políticas restrictivas – Se distingue porque trabaja con base en las restricciones otorgadas, lo que significa que los paquetes que no cumplan estrictamente con las reglas establecidas por el administrador estarán restringidos.

Existen diversas limitaciones que es necesario tomar en cuenta. En primer lugar no se puede proteger a la red de posibles ataques que eviten el punto de operación del firewall. Otro problema que no es posible evitar, es la aplicación de ingeniería social a alguno de los usuarios autorizado de la red.

Todos estos aspectos deben ser tomados en cuenta cuando al momento de instalar un firewall, ya que como es posible apreciar, la efectividad de este sistema de seguridad no sólo radica en el software o hardware utilizado, si no que además es necesario establecer políticas puntuales que establezcan un control preciso del uso de la red.

4.2.- Registro de Eventos (logging)

Quizá uno de los aspectos más descuidados en los sistemas de seguridad es la cuestión de registrar la actividad de la red. Si bien no es una práctica que sea muy difundida, resulta de gran utilidad al momento de registrarse un incidente, ya que brinda una gran cantidad de datos importantes como la procedencia del atacante o el momento en que ocurrió la intrusión.

La recolección de datos es utilizada generalmente para proveer información que ayude a diagnosticar diversos problemas, así como para brindar las pistas del rastro de un atacante. También los datos recabados pueden ser utilizados para determinar la solución y prevención de diversos ámbitos, ya que pueden mostrar situaciones que el administrador en su momento no había detectado.

Afortunadamente, mucho del software que es utilizado en el entorno de la seguridad, como es el caso de firewalls o clientes de correo, cuenta con registro de eventos de manera predeterminada, lo que representa una gran ventaja, ya que no es necesario contar con equipo adicional especializado en este tipo de tareas. Un claro ejemplo es el caso de sistemas Unix, cualquier actividad queda registrada automáticamente en archivos llamados logs.

El servicio que provee el servicio de registro de eventos en la mayoría de estos sistemas operativos es la aplicación syslog, la cual trabaja de manera relativamente simple, los mensajes de la actividad son enviados al demonio designado, y al recibir la información la registra dentro de un archivo de texto.

Generalmente los archivos de registros que son generados de manera automática, tienden a ser complejos en su lectura, por lo que deben ser sometidos a un estudio y análisis en función de entender la información que se encuentra contenida en los mismos con la finalidad de poder encontrar una manera de aplicar los datos recabados.

Para comprender la complejidad de una bitácora, a continuación se muestra un ejemplo de una línea del archivo de registro de eventos “/var/log/pflog” del sistema operativo OpenBSD, un firewall que trabaja a nivel de capa de red:

Jun 01 11:35:57.888954 192.168.1.155.1754 > 62.175.163.20.110: S 11347329:11347329(0) win 64512 <mss 1460,nop,nop,sackOK> (DF)

Donde podemos identificar la siguiente estructura general:

Fecha src > dts Bandera data-sqno : ack Ventana Urgente <Opciones>

- Fecha – Hora en la que ocurrió el evento con el siguiente formato “mes día hora : minutos : segundos.microsegundos”
- src y dts – Direcciones IP y puertos TCP/UDP de las conexiones fuentes y destino respectivamente.
- > - Dirección del flujo de datos.
- Bandera – Posibles combinaciones de las posibles banderas de un datagrama TCP/UDP: S(SYN), F(FIN), P(PUSH), R(RST) y “.” (No Flags).
- data-sqno – Describe el número de la secuencia de datos.
- ack – es el número de byte que se espera recibir en el siguiente extremo de la secuencia.
- Ventana – Es el tamaño de la ventana que advierte el receptor.
- Urgente – Indica que hay datos urgentes en el datagrama.
- Opciones – Son opciones TCP, como puede ser el tamaño máximo del segmento.

Finalmente, en algunas ocasiones al final de la línea se puede denotar una notación extra (DF), la cual es un indicador de no fragmentación.

Como se puede apreciar, es necesario conocer la estructura de las bitácoras y contar con profundos conocimientos de redes a fin de entender lo que se está registrando. En el caso de los servidores, es conveniente hacer un análisis de varias fuentes con el propósito de poder establecer patrones de flujo de paquetes, lo cual puede resultar complicado si no se cuenta con una metodología para llevar a cabo dichas actividades.

4.3.- Criptografía Moderna

La criptografía es la rama de las matemáticas que hace uso de métodos y técnicas que tienen por finalidad el cifrar datos o información a través de algoritmos, los cuales a su vez hacen uso de claves. Como una ciencia aplicada, la criptografía tiene los siguientes objetivos:

- Confidencialidad – La información es leída sólo por las personas autorizadas y a quienes va dirigida la información.
- Integridad de los Datos – La información no debe ser alterada en el transcurso de ser enviada.
- Autenticación – Que sea posible confirmar que el mensaje recibido, haya sido enviado por quien dice ser, o bien que el mensaje recibido el que se esperaba.
- No Rechazo – Que no sea posible negar la autoría de un mensaje por parte del emisor. O bien que el receptor no pueda negar su recepción.

La criptografía sólo hace referencia al aspecto de los códigos y algoritmos empleados para cifrar la información, no de la manera en que estos pueden ser violentados, área conocida como criptoanálisis. Ambas disciplinas se encuentran profundamente ligadas entre sí, y englobadas en la ciencia denominada criptología por lo que es necesario conocerla al momento de crear sistemas de seguridad.

Dentro del criptoanálisis existen tres aspectos que determinan la fortaleza de un algoritmo de cifrado: 1) el tiempo, que está basado en el número de operaciones primitivas que es necesario realizar; 2) el uso de la memoria requerida en el sistema para realizar el ataque; y 3) los datos que se deben manejar, que se traduce como la cantidad de texto plano que debe ser procesado.

A los procedimientos y algoritmos que participan dentro de la criptografía se les conoce en su conjunto como criptosistemas. Una definición más formal es la siguiente: "Los criptogramas se componen de una quíntupla (M, C, K, E, D) donde:

- m representa el conjunto de todos los menajes sin cifrar (que se denomina texto claro) que pueden ser enviados.
- C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el criptosistema.
- E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E^k para cada valor posible de la clave k
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir:

$$D_k (E_k (m)) = m$$ "[16]

Los criptosistemas se dividen en dos grandes vertientes principales, en simétricos y en asimétricos. Debido a que ambos cuentan con ventajas y desventajas entre sí mismos, se opta por utilizar mezclas híbridas de ambos, principalmente en el manejo de firmas o certificados digitales.

Existe otro grupo de funciones criptográficas, conocidas como funciones hash, las cuales son funciones unidireccionales, esto es que dado un mensaje de cualquier longitud generan un resumen del mismo, que teóricamente siempre resulta ser único para cada mensaje, incluso la más mínima modificación genera un resumen

[16] LUCENA López Manuel J. "Criptografía y Seguridad en Computadores", 4ª Edición, Versión 0.7.5, p.30 (http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto)

completamente diferente, por lo que no pueden existir dos documentos con el mismo hash.

Las funciones hash son utilizadas principalmente para obtener huellas digitales asegurando la integridad y autenticidad de los mismos. Los algoritmos más utilizados actualmente son MD5 y SHA-1.

4.3.1.- Criptografía Simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener una comunicación segura entre emisor y receptor siempre y cuando ambas partes hayan realizado previamente un intercambio de la clave correspondiente. El diagrama de ciptosistema se muestra en la figura 4.2. La simetría radica en que ambas partes pueden cifrar y descifrar mensajes utilizando la misma clave.

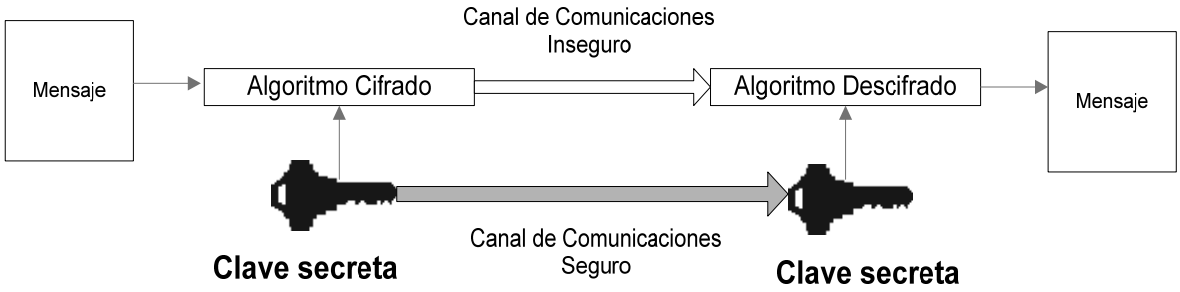


Figura 4.2 – Criptosistema simétrico

Existen dos familias principales de este tipo de criptografía, la primera es la criptografía simétrica de bloques (block cipher) la cual opera bajo unidades definidas de bits, aplicándoles una transformación invariante. En el caso de un mensaje, se toman porciones de longitud fija de dicho mensaje, cada uno de estos bloques es cifrado produciendo bloques del mismo tamaño que el original.

La criptografía simétrica de bloques trabaja en diversos modos de operación, que afectan directamente el grado de confidencialidad e integridad con el que se

deseen manejar los datos. Casi todos, con excepción del modo ECB requieren de un vector de inicialización para comenzar el proceso.

Electronic codebook (ECB)

Es el más simple de los modos de operación. Se dividen los mensajes en bloques y cada uno de ellos es cifrado por separado. Su principal desventaja es que cada bloque cifrado tiene su correspondiente texto en claro, lo que puede ser una guía para un atacante que quiera descifrar el mensaje.

Chiper – block chaining (CBC)

En este modo a cada bloque se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado. Por consiguiente cada bloque depende de todo el texto procesado anteriormente.

Chiper feedback (CFB) y Ouput feedback (OFB)

El cifrado opera como una unidad de flujo, se generan flujos de bloques de claves que son operados mediante XOR y el texto en claro para ser cifrado. Un bit erróneo en el cifrado para OFB genera un bit cambiado en la misma posición, mientras que para CFB un bit erróneo generaría 1+64/m bloques de texto incorrecto, siendo m la longitud de flujo en el que se dividen los bloques.

Counter (CTR)

Convierte una unidad de cifrado por bloques en una unidad de flujo de cifrado. La generación del cifrado es basada en valores sucesivos, un contador, el cual puede ser una función sencilla que produzca una secuencia de números donde los resultados se repitan con poca frecuencia.

La segunda familia es la criptografía simétrica de lluvia (stream cipher) que opera cifrando cada bit de manera individual, y en la cual la transformación de los dígitos sucesivos es variante durante el cifrado. Debido a su naturaleza, resultan menos costosos en el uso de recursos de máquina en comparación con el cifrado por

bloques, aunque resultan ser algoritmos bastantes débiles y susceptibles a ataques si son usados incorrectamente.

La criptografía simétrica de lluvia genera el cifrado en base al estado interno de los procesos del mismo. Esos estados se actualizan básicamente de dos maneras:

-Modo síncrono, los cambios en los estados del proceso del cifrado son independientes del texto plano o el mensaje cifrado. Tanto como el emisor como el receptor deben estar sincronizados para desarrollar los mismos pasos del algoritmo, lo que lo hace susceptible a posibles fallos.

-Modo medio – síncrono, los cambios en los estados tienen cierta dependencia del texto plano, por lo que se procesa una parte de éste y luego se envía al receptor, lo que reduce las probabilidades de error.

Las principales desventajas en este tipo de algoritmos es que, por definición son reversibles ya que se utiliza la misma clave para cifrar y para descifrar. Por otra parte el riesgo de tener una sola clave para realizar los procedimientos lo vuelve extremadamente vulnerable, ya que la clave debe ser compartida entre el emisor y el receptor y a menos que se tenga cuidado en el envió, puede ser interceptada por una tercera parte no autorizada.

Por estos motivos, los algoritmos puramente simétricos no son utilizados generalmente con propósitos de autenticación y no rechazo, para ello regularmente se utilizan funciones hash, como por ejemplo MD5.

4.3.2- Criptografía Asimétrica

En la criptografía asimétrica, se utiliza un par de claves para cifrar y descifrar la información. La primera, la clave privada, es mantenida bajo el resguardo del

propietario y es secreta para los remitentes de los mensajes. La clave pública es distribuida a la comunidad y es dependiente de la clave privada.

Una de las principales ventajas de robustez de los algoritmos asimétricos sobre los simétricos es que no pueden ser cifrados y descifrados con la misma clave, resulta necesaria la interacción de ambas claves para la gestión de los mensajes, lo que reduce el riesgo de que un atacante pueda perpetrar la comunicación al obtener una de las claves. Por otra parte, las claves son números aleatorios de gran tamaño, lo que garantiza la robustez de las mismas.

De acuerdo al servicio que se busca proporcionar, la manera en que funcionan los algoritmos asimétricos son diferentes, aunque en todos se trabaja mediante el principio del uso del par de claves. Existen dos vertientes principales bajo las cuales trabajan estos algoritmos:

- En el uso para asegurar confidencialidad del mensaje
- Para asegurar la identidad de una persona o entidad.

Para los casos de confidencialidad, el emisor cifra el mensaje con la clave pública del receptor y éste a su vez lo descifra con la clave privada, en la figura 4.3 se muestra el esquema de funcionamiento para este caso. De esta manera cualquiera puede enviar un mensaje cifrado, pero sólo el receptor y el emisor que cuentan con la clave privada, pueden conocer el contenido del mensaje.

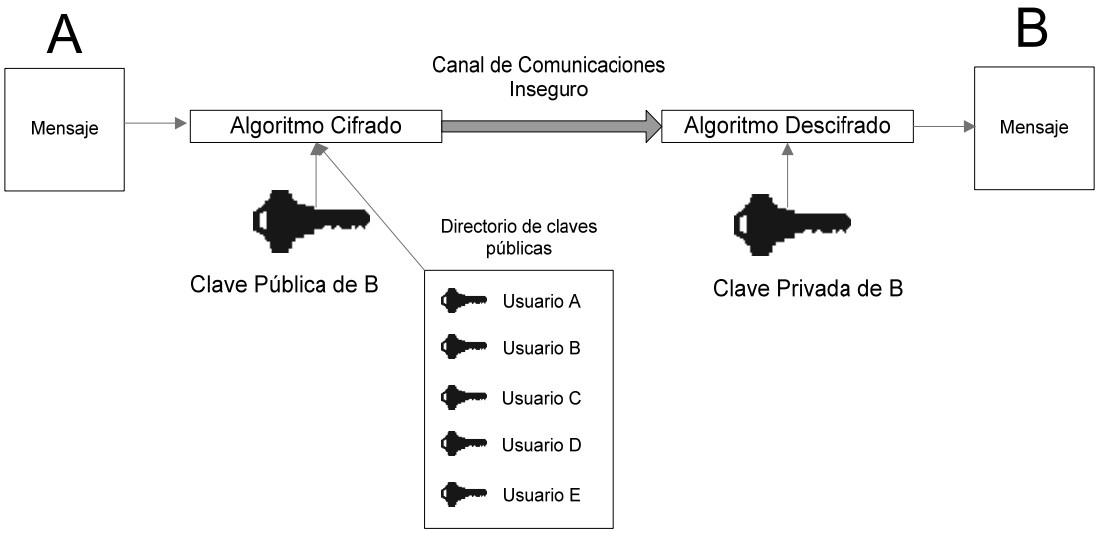


Figura 4.3 – Criptosistema asimétrico para casos de confidencialidad

Cuando se trata de autenticar a la persona, se cifra el mensaje o el resumen del mismo con la clave privada y cualquier persona puede comprobar la procedencia del mensaje utilizando la clave pública del emisor. Se asegura que el mensaje es auténtico porque sólo el emisor verdadero cuenta con la clave privada. Una variante de este aspecto es la firma digital, donde lo que se cifra es el resumen del mensaje.

Si bien, la criptografía asimétrica resulta más robusta que la simétrica, existen ciertas desventajas que deben ser tomadas en cuenta al momento de desear implementar un algoritmo de este tipo:

- Para mensajes y claves de una misma longitud respecto a un algoritmo simétrico, es necesario un mayor tiempo de procesamiento.
- Las claves necesariamente son de mayor tamaño que las simétricas, ya que éstas son generadas de manera aleatoria.
- El mensaje cifrado ocupa un mayor espacio que el original.

4.4.- Clientes y Servidores de Correo

Un programa de cliente de correo es un software especializado en enviar o recibir correo electrónico, y que trabaja conjuntamente con un programa encargado de realizar la transferencia del correo. Actualmente cuentan con una gran variedad de características que fortalecen la seguridad de los usuarios, desde filtros de correo basura hasta herramientas de cifrado.

Debido a que ha crecido enormemente la demanda de correo electrónico tanto en el ambiente laboral como en el personal, han surgido una gran variedad de programas que brindan este servicio y ofrecen una gran diversidad de características tanto como para proteger el correo de posibles intrusiones como para autenticar a los usuarios por diversos método, así como para evitar la propagación del correo spam.

Es en este último ámbito que podemos encontrar una mayor utilidad para los clientes de correo, ya que cada vez resulta más necesario contar con métodos que ayuden a reducir la cantidad de correo no deseado. Por otra parte pueden proporcionar a las empresas medidas de control sobre los mensajes que son enviados y recibidos por los usuarios a fin de que se haga un uso adecuado de los recursos destinados a la producción.

Otra característica que es de gran importancia es el cifrado del correo, así como la utilización de la firma digital. Dependiendo de la criticidad de los mensajes es necesario establecer medidas de seguridad que se cercioren que los datos enviados se encuentren íntegros y el destinatario tenga la certeza que el emisor sea la persona quien se espera.

En algunos clientes de correo es posible evitar la ejecución de código malicioso embebido en el mensaje, puesto que en la gran mayoría de los casos no se permite la ejecución de este tipo de programas al contar con mecanismos que

despliegen exclusivamente los mensajes de texto plano, a menos que el usuario decida habilitar el resto del código.

4.4.1.- Simple Mail Transfer Protocol (SMTP)

SMTP es el protocolo y el estándar oficial utilizado para la transferencia de correo electrónico a través de Internet, ya sea entre computadoras o diversos dispositivos móviles. Se basa en un modelo de comunicación cliente-servidor, en donde los mensajes enviados son cadenas de texto compuestas por caracteres ASCII.

El protocolo SMTP se ejecuta encima de TCP, usando generalmente el puerto 25 del servidor con el cual se establece la conexión. La manera de operar del protocolo es unidireccional, esto es que el emisor puede enviar correos al receptor, pero durante ese período el receptor no puede enviar correos al emisor, sólo respuestas y códigos de estado.

En la figura 4.4, se muestra el modelo de comunicación del protocolo SMTP, se observa la comunicación unidireccional de las máquinas, siendo el emisor un posible intermediario para reenviar el mensaje.

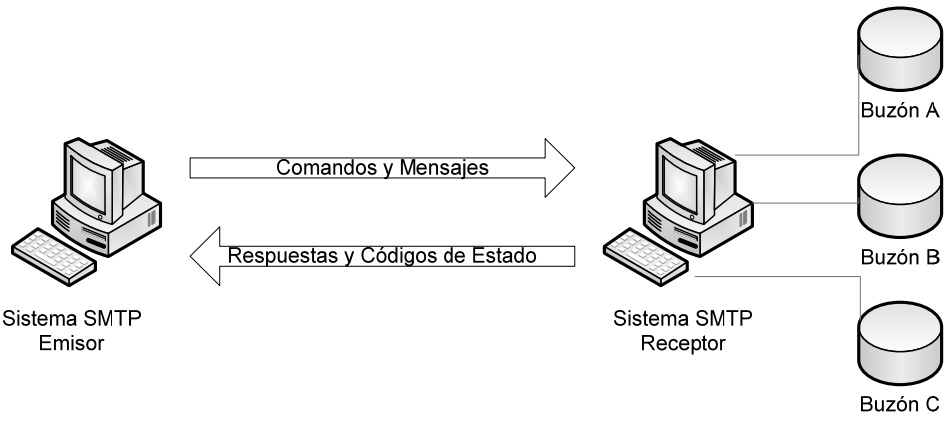


Figura 4.4 – Modelo de Comunicación SMTP

Hay una vulnerabilidad inherente en éste protocolo y es concerniente al hecho de que al utilizar de comunicaciones unidireccionales, no existe ningún tipo de verificación que pueda realizar el emisor con el receptor, lo que hace que se vuelva bastante propenso al spam. Es por ello que se han creando diversas estrategias a fin de reducir éste problema.

Modificar o reemplazar completamente el protocolo SMTP resulta complicado y poco práctico debido al uso tan extendido que tiene actualmente. Un método que puede ser utilizado es enviar una petición de conexión SMTP a la máquina servidor, y esperar algún tipo de respuesta para confirmar la identidad de maquina. Sin embargo existen complicaciones que no permiten la efectividad de éste método, como por ejemplo en el caso de servidores de correo externos que no brindan una respuesta de comunicación.

Otro método utilizado es generar un retardo después de enviar una petición para abrir una sesión con el cliente (conocida como la orden HELO). Muchos bots que envían spam no generan ninguna pausa antes de enviar este aviso, pudiendo ser identificados por los servidores y eliminar la conexión. Desafortunadamente algunos sitios legítimos no utilizan éste método de generar una pausa y son descartados por éste método, además de que este mecanismo no es compatible con el descrito anteriormente.

Finalmente el mecanismo que resulta más conveniente es la utilización de un firewall, y habilitar el puerto 25 para aquellas máquinas que se supone son las únicas que están designadas para funcionar como servidores de correo. Una opción complementaria es poner un límite al tráfico por este puerto, a fin de evitar el envío masivo de correo basura desde una dirección definida.

Como se puede observar, existen diversas medidas de protección para el protocolo SMTP, ya que por si solo no ofrece ninguna garantía de autenticación. Éstas precauciones como se observa no son completamente fiables por lo que se

continúa investigando nuevos métodos que puedan ser sencillos y escalables en su implementación, a fin de que puedan autenticar el correo electrónico a través del mismo protocolo SMTP.

4.4.2.- Secure Socket Layer (SSL) y Transport Layer Securiy (TLS)

TLS y su antecesor SSL son protocolos criptográficos cuyo objetivo es proporcionar comunicaciones seguras a través de Internet para diversos medios que ocupen transferencia de datos como browsers, correos electrónicos o mensajería instantánea. El protocolo TLS está basado en SSL y son similares en la manera de operar.

El diseño del protocolo está orientado para evitar espionaje de datos así como falsificación de los mismos. Usualmente el servidor es el único que se autentica, dejando al cliente con la seguridad de que está estableciendo comunicación con la entidad correspondiente. En caso de requerir que ambas partes se autentiquen mutuamente, se hace uso de una infraestructura de claves públicas asignadas a los clientes.

Los protocolos TLS/SSL están compuestos de dos capas:

- Record Protocol – Es la capa inmediatamente superior a TCP y proporciona una comunicación segura, es la encargada principal de codificar los mensajes usando algoritmos simétricos como DES, aplicándole un MAC (Message Authentication Code) para verificar la integridad y encapsulando los datos para niveles superiores.
- Handshake Protocol – Es la capa superior a la record protocol y es utilizada para gestionar la conexión inicial. El funcionamiento del Handshake Protocol se ilustra en el esquema de la figura 4.5

Figura 4.5 – Funcionamiento del Handshake Protocol

El proceso de comunicación del protocolo TLS/SSL es el siguiente:

- Solicitud de TLS/SSL – Petición para acceder al servidor seguro.
- Handshake – Cliente y servidor se ponen de acuerdo en varios parámetros de la comunicación.
- Intercambio de datos – Los mensajes se cifran con la clave conocida por el servidor y cliente y son enviados al otro extremo donde se descifran y leen.
- Terminación de TLS/SSL – El cliente abandona al servidor y se le informa que terminará la sesión segura para luego concluir con la comunicación.

TLS funciona debajo de protocolos inferiores a la capa de aplicación y encima de los TCP o el protocolo de transporte UDP. Puede agregar seguridad a cualquier protocolo de conexión, aunque es usualmente usado junto con el protocolo HTTP,

para formar el protocolo HTTPS el cual es utilizado en el comercio electrónico. Estas aplicaciones utilizan certificados digitales para verificar la autenticidad de los sitios.

Una aplicación más especializada es en el uso de túneles para comunicación segura, es decir, establecer comunicaciones directas entre un usuario y un servidor aún cuando se utilice una conexión de carácter público como lo es Internet, y a las cuales se les conoce como redes privadas virtuales (VPN por sus siglas en inglés).

4.5.- Certificados Digitales

Un certificado digital es un documento electrónico que utiliza una firma digital a fin de poder garantizar la identidad de una entidad por medio de una clave pública. Usualmente el certificado digital es emitido por una empresa certificadora autorizada, aunque en una red de confianza la firma puede ser de cualquiera de los usuarios.

"Los certificados digitales se clasifican en tres vertientes principales:

- Clase 1 – para individuos, requeridas para correo electrónico.
- Clase 2 – para organizaciones, para las cuáles es necesario pruebas de identidad.
- Clase 3 – para servidores y firmas de software, para los cuáles la identificación y la revisión de la identidad es hecha por la empresa certificadora."[17]

[17]Fuente: Verisign, Inc

Todo certificado tiene un período de vida útil, a fin de garantizar la integridad del mecanismo, asegurando la constante renovación de las claves en caso de que así se requiera. Todas estas medidas garantizan la robustez del certificado digital ante el usuario, quien dependiendo de la importancia de los datos puede resultar crítico contar con una garantía.

De acuerdo al estándar X.509 del Sector de Normalización de las Telecomunicaciones de la UIT (ITU-T por sus siglas en inglés), la estructura que debe tener cualquier certificado digital es la siguiente:

-Certificado
- -Versión
- -Número de Serie
- -Algoritmo de Identificación
- -Institución Certificadora
- -Validez
  - -Fecha de Inicio
  - -Fecha de Terminación
- -Sujeto
- -Información de la clave pública del sujeto
  - -Algoritmo de la clave pública
  - -Clave Pública del sujeto
- -Identificación única del la institución certificadora (opcional)
- -Identificación única del sujeto (opcional)
- -Extensiones (opcional)

-Algoritmo de la firma del certificado

-Firma del certificado

Existen diversas empresas certificadoras que trabajan de manera multinacional. La gráfica de la figura 4.6 muestra un estudio realizado por la compañía Netcraft

en junio de 2005 en relación a la distribución del mercado entre las principales compañías certificadoras.

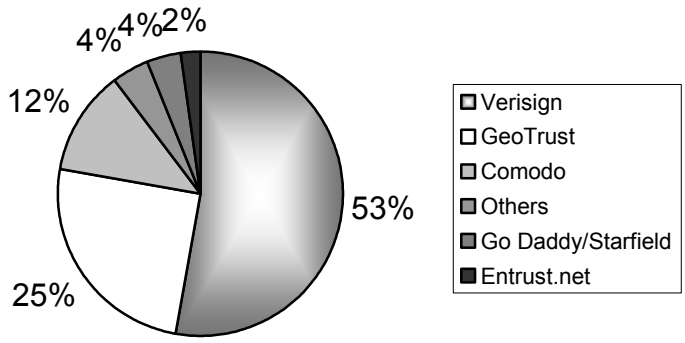


Figura 4.6 – Distribución del mercado de certificados digitales[18]

Existen dos organizaciones importantes que no aparecen registradas en el estudio, CAcert.org y StartCom Certification Authority, las cuales brindan el servicio de manera gratuita.

4.5.1- Firma Digital

Una firma digital es una secuencia de bits que son añadidos a una pieza de información cualquiera, y que permite garantizar su autenticidad sin depender de proceso de transmisión utilizando un algoritmo asimétrico. Es posible hacer una analogía con la firma manuscrita, ya que cumple con características similares.

"Requisitos de la firma digital

a) fácil de generar
b) irrevocable, no rechazable por su propietario.

[18]Fuente: Netcraft (May-Jun 2005)

c) única, sólo posible de generar por su propietario.
d) fácil de autenticar o reconocer tanto por el propietario como por los usuarios receptores.
e) depender del mensaje y autor."[19]

Las firmas digitales solamente pueden utilizar algoritmos asimétricos. Por otro lado las firmas digitales que trabajan con algoritmos asimétricos tienen una alta fiabilidad y puede tener una vida duradera bastante extensa.

Por otro lado, la aplicación de un algoritmo asimétrico requiere una mayor cantidad de recursos en comparación con un algoritmo simétrico, por lo que se opta por obtener un resumen del mensaje que se desea firmar por medio de una función hash, el cual comprende entre 128 y 160 bits. Este resumen obtenido es el que se firma, volviendo más eficiente el uso de los algoritmos asimétricos.

Por consiguiente los métodos que se utilizan generalmente para manejar firmas digitales son aquellos basados en algoritmos asimétricos, los cuales trabajan de la siguiente manera:

- El emisor calcula el código hash del documento.
- Con la clave privada cifra el hash obtenido anteriormente.
- Envían el documento y el hash cifrado, éste es la firma digital.
- El receptor, que debe contar con la clave pública del emisor, descifra la firma digital.
- Calcula el código hash del documento y es comparado con el que se obtuvo del código descifrado, ambos deben ser iguales.

Una carencia inherente en la firma digital es que no es posible tener certeza de la fecha y hora en que los mensajes fueron firmados, por consiguiente, un mensaje

[19] RAMIÓ Aguirre Jorge, "Libro Electrónico de Seguridad Informática y Criptografía", Universidad Politécnica de Madrid, España, 2006, p. 775 (http://www.criptored.upm.es/guiateoria/gt_m001a.htm)

usando exclusivamente este mecanismo no puede ser usado como referencia al momento en que éste haya sido enviado. Para tales casos es necesario usar otros métodos, como por ejemplo sellos de tiempo.

4.5.2- Pretty Good Privacy (PGP)

PGP es un proyecto iniciado por Phillip Zimmerman, cuya finalidad ha sido brindar una herramienta que permita ofrecer seguridad y privacidad cifrando y descifrando mensajes de manera robusta y eficaz. PGP se convirtió en un estándar internacional (RFC 2440) y es utilizado por diversos programas en la actualidad.

PGP trabaja con una combinación de criptografía simétrica con asimétrica, ofreciendo una enorme facilidad al usuario final para poder gestionar sus claves pública y privada. En primera instancia el mensaje es cifrado usando un algoritmo simétrico con una clave aleatoria generada durante la sesión, y posteriormente codifica dicha clave haciendo uso de la clave pública del destinatario. La figura 4.7 muestra un esquema de cómo funciona el cifrado de los mensajes:

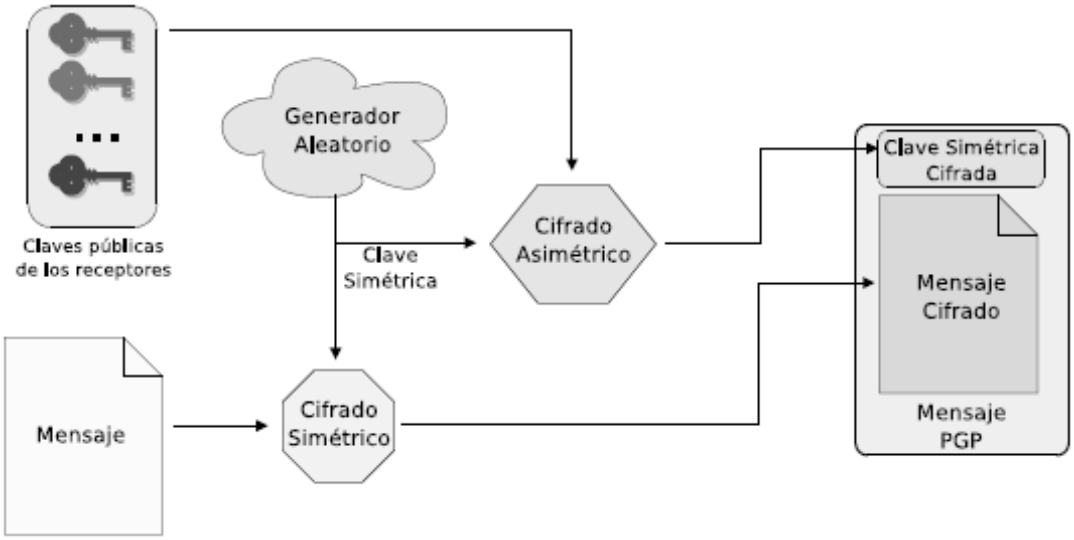


Figura 4.7 – Codificación de un mensaje PGP[20]

[20] LUCENA López Manuel J. "Criptografía y Seguridad en Computadores", 4ª Edición, Versión 0.7.5, p.240 (http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto)

El receptor que recibe el mensaje utiliza su clave privada para descifrar la clave de sesión y finalmente utilizar ésta para poder descifrar el mensaje. El uso de ésta técnica resulta bastante importante, porque como se ha visto, la velocidad de procesamiento entre un algoritmo asimétrico y un simétrico resulta bastante considerable.

PGP almacena las claves en estructuras conocidas como anillos, las cuales son una colección de claves almacenadas en un archivo. Se cuenta con dos tipos de anillos, uno especial para las claves públicas y otro para las claves privadas. La información contenida en cada uno de los archivos comprende además de la secuencia binaria correspondiente al algoritmo, una serie de datos como la identidad del usuario, la fecha de expiración, la versión de PGP con que fue creada y la denominada huella digital, cuyo ejemplo se muestra a continuación:

4E0D C6F6 2C1A 24CD C3C5 4146 B468 E820 BD53 CBC4

La huella digital resulta de bastante utilidad para poder corroborar la autenticidad de una clave. Como se puede apreciar, consiste en una serie de números hexadecimales con una longitud considerable que permite asegurar la autenticidad de una clave.

Actualmente existen diversas variantes del algoritmo, siendo especialmente reconocido el desarrollado bajo el proyecto GNU, GnuPG (GNU Privacy Guard), que funciona en una gran cantidad de plataformas y emplea algoritmos de libre distribución y presenta una estructura que lo vuelve fácilmente extensible. Si bien surgió una vulnerabilidad durante su desarrollo al intentar hacer más eficiente uno de los métodos éste ha sido corregido en las últimas versiones.

4.6.- Cómputo Forense

El cómputo forense es una disciplina de seguridad informática aplicada en los sistemas de cómputo, con la cual se obtiene información sobre el uso que se ha hecho tanto del sistema como de la información que se maneja, almacena o transmite en el mismo. Se hace uso de software especializado y de diversos conocimientos en diversas áreas de la computación para determinar los comportamientos y acciones realizadas por intrusos.

En el ámbito académico, el cómputo forense es la aplicación de técnicas científicas y analíticas en el campo de la informática para identificar, preservar, analizar y presentar evidencia de delitos que sea válida en un proceso legal o dentro de un proceso de investigación interno en una organización.

El cómputo forense es una disciplina relativamente nueva que está en desarrollo en nuestro país. Uno de los países que ha tenido grandes avances en este terreno es Chile, a través de su brigada de cibercrimen, éste fue el primer país de la región en contar con una policía enfocada al crimen cibernético. A nivel del continente, EUA representa la punta de lanza en esta disciplina; pero cabe destacar que existen centros de investigación y cómputo forense muy grandes contra el terrorismo a nivel mundial.

El cómputo forense sigue una metodología para poder hacer recolección y análisis de la evidencia. Los pasos básicos que se deben seguir en el proceso son los siguientes:

1.- Adquirir las evidencias sin alterar ni dañar el original. La forma ideal de examinar un sistema consiste en examinar una copia de los datos originales. El sistema debe permanecer como se encontraba después de haberse detectado el ataque, esto es si se encontraba encendido debe mantenerse así, lo mismo si se encontraba apagado. Es importante tener en cuenta que no se puede examinar un

sistema presuntamente comprometido utilizando las herramientas que se encuentran en dicho sistema pues éstas pueden haber sido afectadas.

2.- Comprobar que las evidencias que fueron adquiridas y las cuales van a ser la base de la investigación, son idénticas a las generadas por el delincuente en la máquina afectada. Las técnicas y herramientas de control de integridad que mediante la utilización de una función hash generan una huella electrónica digital de un archivo o un disco completo resultan fundamentales para este tipo de comprobación.

3.- Analizar los datos sin modificarlos. En este punto, es crucial proteger las evidencias físicas originales trabajando con copias idénticas de forma que en caso de error se pueda recuperar la imagen original y continuar con el análisis de forma correcta. Se recomienda la realización de dos copias de los discos originales, los cuales deben ser clones realizados bit a bit del dispositivo original ya que los respaldos normales no copian archivos que hayan sido eliminados, ni tampoco determinadas partes de los discos que pueden contener pistas importantes para el desarrollo de la investigación.

"Las evidencias digitales presentan una serie de ventajas sobre las evidencias físicas. Estas ventajas son:

- Pueden ser duplicadas de forma exacta, pudiendo examinarse la copia como si fuera el original. Si alguien intenta destruir las evidencias se pueden tener copias igualmente válidas lejos del alcance del criminal.
- Con la utilización de herramientas adecuadas es fácil determinar si la evidencia ha sido modificada o falsificada comparándola con la original.
- Es relativamente difícil destruir una evidencia digital. Incluso borrándola puede ser recuperada del disco."[21]

[21] CANELADA Oset Juan Manuel, "Análisis Forense de Sistemas Linux", Universidad Autónoma de Madrid, 2004, p.3 (htt://crl.iic.uam.es/descargas_web/cursos_verano/20040801/JuanMa_Canelada/Analisis_forense_de_sistemas.pdf)

UNAM-CERT es el primer equipo de respuesta a incidentes con reconocimiento internacional es nuestro país. Fundada en el año 2000 por la DGSCA (Dirección General de Servicios de Cómputo Académico), la UNAM-CERT es un equipo de especialistas en seguridad en cómputo que atiende a instituciones de cualquier tipo, que han sido víctimas de algún ataque tanto en sus sistemas informáticos, además publica periódicamente información actualizada sobre alertas y vulnerabilidades, implantación de políticas, elabora análisis de riesgos y realiza investigación dentro de esta área para contribuir a hacer, cada día, más seguros los sistemas y las redes.

Los incidentes que se atienden son cada vez más importantes, los casos más frecuentes ocurridos en la UNAM que han sido detectados y atendidos son:

- Abuso de recursos para afectar a otras redes.
- Envío de correo spam.
- Sospechas de personas que acceden a archivos personales a los que no tienen permiso.

Actualmente se atienden incidentes con implicaciones más importantes dentro de la Universidad, se colabora con entidades gubernamentales encargadas de la investigación de delitos informáticos, participa en monitoreos mundiales sobre actividad maliciosa y se trabaja de manera coordinada con instituciones financieras afectadas por problemas de fraudes.

Entre los casos atendidos en México sobre esta materia por parte del UNAM-CERT están:

- Fraudes. Transferencias bancarias a través de sistemas de banca en línea.
- Presidencia de la República, ataque de negación de servicio.
- En algunos casos se pudo castigar a los culpables.

Capítulo 5

Propuesta de Prácticas de Seguridad Informática

Capítulo 5
Propuesta de Prácticas de Seguridad Informática

Como se ha explicado y mostrado a lo largo de los capítulos anteriores, existe una urgente necesidad de poder contar con personas capacitadas en el área de seguridad informática y que a su vez conozcan las herramientas necesarias para hacer frente a las diversas amenazas que existen actualmente en dicho campo. Es por tales motivos, que en el presente capítulo se muestra una propuesta de prácticas para el Laboratorio de Redes y Seguridad, las cuales fueron diseñadas basándose en la información descrita anteriormente.

Si bien, no es posible abarcar en su totalidad todos los aspectos relacionados a la seguridad informática, y mucho menos tratar cada una de las particularidades concernientes a dicho tema, las prácticas se han establecido basándose en los principales focos indicadores más destacados y de importancia crítica para cualquier tipo de industria, tanto en el sector público como privado.

Se ha resaltado la importancia de evitar en su totalidad el uso de programas de procedencia ilícita (piratas), optando por la utilización de herramientas con licencia o de uso libre, lo cual tiene dos finalidades primordiales:

- Evitar delitos de derechos de autor teniendo siempre, si así se requiere, versiones de software actualizado y de alta confiabilidad, respaldado en la mayoría de los casos por una comunidad activa.

- Hacer que los alumnos sean conscientes de que existen alternativas al software de propietario para cualquier tarea que requiera desarrollarse dentro del área profesional de la carrera.

Por otra parte fue necesario adaptar las prácticas a las condiciones con que se cuentan en el Laboratorio de Redes y Seguridad por lo que además de la realización de diversas pruebas, se impartieron un par de talleres con alumnos pertenecientes a la carrera de Ingeniería en Computación, lo cual resultó ser fundamental para la realización de diversas correcciones.

5.1.- Planteamiento inicial

El primer planteamiento fue que los temas que se eligieran estuviesen basados en las necesidades actuales de la industria y de las instituciones. Es por ello que se tomó como base los datos planteados durante los capítulos anteriores, buscando un modo eficiente para que los alumnos puedan realizar las actividades descritas en las prácticas de manera individual y sin la necesidad de tener que invertir en la compra de equipo adicional o software propietario.

Si bien, algunos temas quedaron fuera del esquema de prácticas planteado, se buscó condensar en la medida de lo posible la mayor cantidad de información vista tanto en la parte teórica del área de seguridad informática así como en los problemas más recurrentes que afectan a la sociedad actualmente, y que en diversas ocasiones resulta complicado tener un acercamiento a dichas dificultades de manera individual.

Por otra parte se desarrolló una práctica cero, la cual es una introducción a los sistemas Unix, particularmente a Linux, ya que por experiencia se ha notado que no todos los alumnos de la carrera de Ingeniería en Computación cuentan con los conocimientos necesarios para el manejo de dicho sistema operativo, siendo que

actualmente es una necesidad dentro del campo laboral, resultando indispensable tener conocimientos sobre el manejo de dicho sistema.

Por último fue necesario considerar las condiciones del equipo de laboratorio, ya que las máquinas con que se cuentan resultan tener diversas características de capacidad, por lo que el software que se utiliza debe ser capaz de poder funcionar en los equipos sin la necesidad de hacer modificaciones extras ni comprar material adicional.

5.1.1- Criterios para la elección de temas

Originalmente se tenían planteados ocho temas principales que se distribuirían a lo largo de todas las prácticas que se realizaran. Los temas planteados fueron:

- Manejo de contraseñas.
- Firewalls
- Clientes de correo
- Firmas Digitales y Cifrado de Correo
- Cómputo Forense
- SSH seguro.
- Monitoreo de Redes.
- Seguridad en Sistemas y Bases de Datos.

Estos temas fueron seleccionados originalmente basándose en los boletines publicados por DGSCA[22], noticias generales sobre seguridad informática, datos estadísticos recabados a lo largo de la investigación, experiencia personal a lo largo de la carrera y diversas consultas realizadas a la M. en C. Ma. Jaquelina López Barrientos.

[22] Fuente: http://biblioteca.dgsca.unam.mx/cu/productos/boletines/

De manera inicial se planteó una práctica correspondiente para los temas de SSH seguro y monitoreo de redes, pero debido a que dentro del laboratorio ya habían sido cubiertos por prácticas similares, se decidió eliminar estos temas debido a que sería redundante volver a tratarlos nuevamente.

En el caso del tema de clientes de correo, se incluyó posteriormente una investigación sobre spam y sus efectos en el costo para las instituciones. Originalmente la práctica estaba conformada también por el cifrado de mensajes y creación de la firma digital, pero debido a la extensión de la misma, se optó por trabajarla en dos partes, lo que permitió ahondar más en los temas.

Por otra parte, los temas referentes al cómputo forense, fueron desarrollados con base en el trabajo de investigación realizado durante el curso de la materia Seminario de Ingeniería en Computación por parte de Luis Gerardo Tejero Gómez. Debido a que se trata de un tema relativamente nuevo en nuestro país, resulta fundamental adentrar a los alumnos de las nuevas generaciones en el cómputo forense, a fin de que eventualmente se convierta en una herramienta de uso común para cualquier profesionista que trabaje en el campo de la seguridad informática.

Uno de los temas que fue descartado por razones de seguridad y control fue el de “virus informáticos”. Las principales razones para que dicho tema no fuera incluido dentro de las prácticas fue que resulta bastante complejo poder tener una simulación de un ataque real, ya que un virus en los sistemas Windows usualmente resulta ser bastante agresivo y fácil de propagar, por lo que establecer un procedimiento repetitivo requeriría medidas extras de seguridad.

En sistemas Linux, sus efectos no resultan tan obvios y dañinos, pero a su vez no es permisible infectar los equipos deliberadamente ya que se corren diversos riesgos a la seguridad de la red no sólo del laboratorio, sino de todos aquellos equipos que tengan contacto con ella, siendo el mismo caso para Windows, en el

que se requerían medidas extras de seguridad. Probablemente la mejor solución sería tener un equipo aislado de la red, pero eso hubiera limitado en gran medida la interactividad de los alumnos dándose restricciones de una aplicación real.

Para el tema de seguridad en bases de datos, se utilizó un servidor standalone, el cual se puede instalar y desinstalar en cualquier máquina y no necesita ningún tipo de conexión en red para poder trabajar. La práctica abarca diversos temas en si relacionados a la seguridad en bases de datos, como es el uso de cifrado md5 para las contraseñas, así como maneras de prevenir inyección de código SQL.

Por otra parte, para la depuración de los temas que se tenían originalmente, la realización de dos talleres permitió integrar tópicos no manejados en las prácticas originales, pero que resultaban importantes desde el punto de vista de los participantes de dichos talleres. En las versiones finales se incluyo la mayor parte de las sugerencias recabadas, así como algunos tópicos que fueron sugeridos posteriormente para complementar los temas tratados en la teoría.

5.1.2- Criterios para la elección de software

Uno de los primeros aspectos que se consideraron para elegir el software es que éste fuera principalmente software libre, a fin de evitar el uso de programas con licencia privada y por consiguiente con costo económico, o bien, hacer uso de programas ilícitos, lo cual conlleva a diversas violaciones a la ley, que son necesarias evitar.

“El software libre proporciona la libertad de:

- Ejecutar el programa, para cualquier propósito;
- Estudiar el funcionamiento del programa, y adaptarlo a sus necesidades;
- Redistribuir copias;

- Mejorar el programa, y poner sus mejoras a disposición del público, para beneficio de toda la comunidad. "[23]

Es importante no confundir con la definición de Open Source, que si bien, se refiere a la libertad de modificación del código, no necesariamente implica la libertad de redistribución. Por consiguiente, para el desarrollo de las prácticas se buscó que el software que se utilizara siguiera preferentemente estos principios,

El siguiente criterio para seleccionar el software fue que figurara dentro de diversos medios, es decir, que existiera cierto grado de reconocimiento tanto por publicaciones, foros enfocados a la seguridad de sistemas, sitios webs especializados, etcétera. Del mismo modo, se revisó que se contara con suficiente soporte en línea, a fin de tener tanto información de su funcionamiento, como la facilidad de que éste pudiera estar disponible fácilmente en Internet.

Con base en esto, una primera tentativa del software planteado fue el siguiente:

- <<Back | track 2 – Sistema Operativo que contiene diversas herramientas para la realización de pruebas de seguridad en sistemas y redes.
- John the Ripper – Programa para auditar contraseñas en diversos sistemas operativos.
- Pwdump – Herramienta para el volcado de passwords en Windows NT.
- LCP – Herramienta para auditar y recuperar passwords de Windows.
- ZoneAlarm (versión gratuita) – Firewall de uso personal, con reconocimiento en diversas publicaciones.
- Coyote Linux – Firewall de distribución gratuita que trabaja con una cantidad mínima de recursos en el sistema.
- Thunderbird – Cliente de correo producido por Mozilla, con gran flexibilidad de uso.
- GPG4win – Variante del programa GPG en su versión para Windows.

[23] Fuente: http://fsfeurope.org/

- Autopsy – Herramienta para la realización de cómputo forense.
- Sleuthkit – Front end para Autopsy que trabaja por medio de un browser.
- Wireshark – Herramienta para captura y análisis del flujo de información en redes de computadoras.

Posteriormente, se realizaron algunas pruebas dentro del Laboratorio de Redes y Seguridad de la Facultad de Ingeniería, encontrando ciertas complicaciones dentro del esquema de seguridad del mismo, por ejemplo, para el caso de los programas para auditar las contraseñas, fue necesario descartar LCP y Pwdump debido a que su funcionamiento resultaba poco práctico si se planteaba requerir probar diversas contraseñas.

Para el caso de Coyote Linux, si bien es un software robusto y fiable, fue descartado por su complejidad en el manejo, además de tratarse de un firewall que trabaja en capa de red, necesita un equipo especializado en la tarea de filtrado de paquetes, por lo que resultaba complicado establecer una metodología que fuera didáctica para los alumnos.

Finalmente, el programa Wireshark que se planteaba fuera utilizado en la práctica de monitoreo de redes, fue descartado por la razón de que la práctica en sí resultaba similar a otra ya existente. Posteriormente, y después de realizado el primer taller de pruebas, y tras la creación de las nuevas prácticas, se incluyeron los siguientes programas adicionales a fin de complementar las prácticas ya propuestas:

- Core Force – Firewall de uso libre, que basa su funcionamiento en la mecánica propuesta para OpenBSD.
- XAMPP – Servidor standalone que cuenta con una gran flexibilidad, que cuenta con una amplia documentación y facilidad de uso.

Finalmente el último punto que consideró para la selección del software, es que éste pudiera ser instalado con relativa sencillez en los equipos del laboratorio, a fin de que durante la realización de las prácticas, fueran los mismos alumnos quienes pudieran encargarse no sólo de manipular el software una vez instalado, sino que a su vez pudieran instalarlo y configurarlo personalmente.

5.2.- Realización de pruebas

Una vez que se finalizó con el planteamiento teórico de las prácticas, y se hubo corroborado el funcionamiento en una computadora personal, se realizaron diversas pruebas en el laboratorio de Redes y Seguridad a fin de verificar que lo propuesto en las prácticas era viable y aplicable en el entorno de trabajo donde se desarrollarán las prácticas.

Por consiguiente se propuso en primera instancia realizar diversas pruebas de manera individual en diversos equipos buscando encontrar las fallas principales en el funcionamiento de prácticas o bien corregir y prevenir posibles problemas con el material utilizado. Posteriormente se realizaron un par de talleres con alumnos pertenecientes a la carrera, a fin de poder comprobar la efectividad de las prácticas en un entorno real.

Es con base en este último punto que se realizaron la mayoría de las correcciones y mejoras al material con el que se contaba en el momento, ya que la retroalimentación recibida a través de los comentarios de los participantes ayudó en gran medida a detectar fallos y carencias que de manera aislada no podrían haberse mostrado de forma evidente.

Las prácticas que finalmente quedaron para uso del laboratorio, así como parte del material que es necesario para la elaboración de las actividades descritas en las

mismas, se anexan a este documento y quedan a disposición de la UNAM para que sean dispuestas como mejor convenga.

5.2.1- Verificación de Funcionamiento en Laboratorio

Para la verificación del funcionamiento de cada una de las prácticas, se realizaron diversas pruebas en el Laboratorio de Redes y Seguridad de la Facultad de Ingeniería, con la finalidad de que lo propuesto en las prácticas pudiera ser utilizado cabalmente en el espacio que se tiene designado para dichas actividades.

En primera instancia se verificó que los programas pudieran ser instalados correctamente en las máquinas con las que se cuenta en el laboratorio. Aparte de observar el correcto funcionamiento de los programas instalados, se tomó en cuenta que el tiempo necesario para su instalación no resultará excesivo, en especial en aquellas computadoras que cuentan con menos capacidad de procesamiento y memoria.

Posteriormente se realizó lo descrito en cada una de las prácticas en distintas máquinas al azar dentro del laboratorio, tomando en consideración que el desempeño que debía presentarse en las máquinas debería ser bastante similar, a fin de evitar que al momento de realizar la práctica, no existieran retrasos graves que dificultaran las actividades en grupo.

Uno de los principales problemas encontrados para la realización de las prácticas, se presentó en la correspondiente a cómputo forense, ya que debido a que se trabaja con la imagen de un disco corrompido y con un liveCD, es necesario contar con un medio externo que permitiera extraer las imágenes del disco comprometido con las que se deben realizar las pruebas. La solución encontrada fue copiar las imágenes al disco duro de la computadora y montarlas a partir desde esa ruta.

Otro de los problemas encontrados es que la distribución de Linux instalada en los equipos de laboratorio (Fedora 3) presentaba diversas complicaciones para instalar algunos de los programas que fueron planteados a lo largo de la práctica, principalmente por la falta de algunas librerías. Por consiguiente, se optó por trabajar directamente usando el liveCD que se proporcionó y que contiene el software necesario para trabajar con la finalidad de evitar complicaciones al momento del desarrollo de las prácticas.

En su mayoría, las prácticas fueron probadas antes de la realización de los talleres, salvo excepciones en donde se buscó experimentar algunas herramientas que no habían sido probadas con anterioridad. Posteriormente, y al observar los resultados de los talleres, se realizaron las correcciones pertinentes en las prácticas y fueron probadas nuevamente en el laboratorio, quedando por concluido el trabajo correspondiente a la implementación de dichas herramientas.

5.2.2- Talleres impartidos

Fueron impartidos dos talleres, los cuales tenían como principales objetivos brindar conocimientos referentes a la seguridad informática a los asistentes a ellos y por otra parte, recibir una retroalimentación de las prácticas planteadas así como recabar información que permitiera mejorar y corregir ciertos aspectos de las mismas.

El primer taller se realizó del 15 al 18 de Enero del 2007, teniendo una duración total de 10 horas en cuatro días, en los que se mostraron los conceptos que hasta ese momento se habían trabajado y se realizaron las pruebas pertinentes. La participación de las personas que asistieron a dicho taller resultó de vital importancia para poder realizar diversos cambios y mejoras que posteriormente serían probados nuevamente.

En este primer taller se invitó a que participaran compañeros y personas conocidas, ya que era importante en primera instancia tener gente con cierto nivel de conocimientos que pudieran realizar observaciones precisas a los temas planteados y que aportaran nuevas ideas tanto al uso de herramientas, así como recomendación de temas que en su momento no habían sido incluidos. De este primer taller se obtuvieron los siguientes comentarios:

- Crear una práctica introductoria al sistema Linux.
- Ahondar en el manejo de firewalls y mostrar otras herramientas disponibles.
- Incluir aplicaciones de algoritmos de cifrado.
- Incluir previos en las prácticas.
- Crear una práctica referente a la seguridad en la programación.
- Diversas correcciones en el planteamiento de los temas.

De estos comentarios se trabajó en la generación de algunas prácticas adicionales, así como en la inclusión de diversos tópicos sugeridos durante éste primer taller. Así mismo se corrigieron algunos puntos que resultaban redundantes y poco concisos, aunque hay aspectos que debieran profundizarse en una siguiente versión de las prácticas aquí elaboradas.

El segundo taller, fue realizado del 26 de Enero al 2 Febrero del 2007, como parte de las Jornadas de Ingeniería en Computación, y teniendo en esta ocasión alumnos de los últimos semestres de la carrera, quienes participaron de manera voluntaria siendo la única condición que se encontraran cursando por lo menos el séptimo semestre de la carrera; cabe mencionar que fue un taller con una duración total de 10 hrs. en cinco días.

Las prácticas presentadas fueron finalmente la versión corregida y actualizada de las realizadas en el primer taller, salvo correcciones menores que se hicieron posteriormente. Al igual que en el primer taller, después de presentarse y trabajar

utilizando el material proporcionado en las prácticas, se recabaron comentarios y sugerencias sobre los temas tratados y las herramientas utilizadas.

En general, el material que se utilizó fue aprobado por los asistentes salvo detalles que posteriormente fueron corregidos, concluyendo que las prácticas resultaban convenientes y apropiadas para la enseñanza de temas relacionados a la seguridad en el ámbito de las redes y la informática.

Es finalmente con las correcciones realizadas a partir de la información recabada en este taller que se concluyó con la elaboración de las herramientas para la enseñanza de seguridad informática.

5.3.- Descripción de las prácticas

Los formatos así como los contenidos de las prácticas se encuentran en el CD anexo del presente trabajo, por lo que a continuación se describe de manera general diversos aspectos encontrados en cada una de ellas, así como diversas explicaciones de los puntos más sobresalientes en cada uno los temas contenidos. Del mismo modo se da una reseña general de la finalidad que tienen los diversos ejercicios planteados a lo largo de dichas prácticas.

La metodología planteada en cada una de las prácticas es que se puedan observar casos prácticos de seguridad, así como fomentar las habilidades necesarias para manejo de todo tipo de software relacionado con la seguridad informática y hacerlo de manera responsable. Por consiguiente también se tomó en cuenta que los alumnos participantes en los talleres mencionados tenían diferentes grados de habilidad, así como el conocimiento previo con el que cuentan resulta bastante diverso.

Dicho aspecto que será resuelto al ser realizadas estas prácticas en el Laboratorio de Redes y Seguridad ya que los estudiantes que las realizarán serán del módulo de Redes y Seguridad y estarán cursando asignaturas de Seguridad Informática, por lo que se espera que el nivel de desempeño y aprovechamiento sea relativamente el mismo en los alumnos que asistan al laboratorio.

La duración de las prácticas también fue un factor considerado al momento de establecer la cantidad de actividades en cada una de las prácticas, tomando en cuenta que se buscaba cierta sencillez, pero no por eso simpleza, al momento de diseñar las prácticas ya que como se mencionó anteriormente se buscó que las actividades puedan ser reproducidas constantemente y que no fuera necesario adquirir equipo adicional para la realización de las mismas.

.

En su mayoría, las prácticas han sido ideadas y diseñadas para una duración de alrededor de una hora teniendo entonces que considerar los tiempos establecidos para los laboratorios, siendo que el profesor pueda dar una breve introducción al tema y resolver diversas dudas al final de cada práctica.

Por otra parte, el uso de diferentes sistemas operativos, para el caso de las prácticas (tanto Windows como Linux), hace que el alumno comprenda la importancia de considerar la gama de posibilidades que existen, además de que cada uno de los sistemas operativos presenta ventajas y desventajas. En el caso de Windows resulta el sistema más utilizado pero es a su vez el que cuenta con mayores deficiencias de seguridad, por otra parte el sistema operativo Linux resulta mucho más robusto pero es menos popular que su contraparte.

Finalmente se intentó abarcar la mayor cantidad de temas posibles relacionados a seguridad informática, pero debido a que se trata de un tema demasiado extenso, se hizo la mayor síntesis de los mismos, abarcando de manera general los aspectos más sobresalientes, y pensando en que la realización del previo como la

entrega de reportes abarcarían en la medida de los posible cada uno de los tópicos planteados.

5.3.1- Práctica 1 – Establecimiento de Contraseñas Robustas

La práctica se enfoca en demostrar que no importa la fortaleza de un algoritmo para cifrar una contraseña, si ésta no cumple con ciertos requerimientos básicos de seguridad, puede ser fácilmente obtenida por medio de algún programa dedicado a ello. Ya que las contraseñas resultan ser cifradas de manera mucho más robustas para los usuarios dentro de un sistema Unix que en sistemas Microsoft se optó por utilizar Linux en esta práctica.

Por otra parte, la facilidad que se tiene para crear usuarios, cambiar su contraseña por medio de la línea de comandos, resulta más didáctico, además de hacer que el alumno utilice este sistema para hacer modificaciones al sistema, fomentando la habilidad de trabajar por medio de línea de comandos. Por otra parte, la manera en que los diversos programas enfocados en auditar contraseñas, resultan ser más prácticos en el sistema elegido.

En el caso de Windows, para descifrar la contraseña de un usuario es necesario ubicar el archivo “SAM” (Security Account Manager), dentro de la carpeta %systemroot%system32config, que contiene los hashes de las contraseñas y el cuál sólo puede ser accedido cuando el sistema operativo no ésta funcionando. Por consiguiente es necesario acceder al disco de manera externa, copiar el archivo, y usar el programa correspondiente para romper la contraseña.

Por otra parte, en sistemas Linux, el archivo que contiene los hashes de las contraseñas está ubicado en /etc/shadow, y no es necesario que el equipo se encuentre apagado para que pueda ser accedido, aunque sí deben contarse con privilegios de root para poder tener acceso a él. Debido a esta facilidad, se optó

por este sistema operativo, ya que es posible probar diversas contraseñas de manera rápida.

Ya que actualmente se utilizan principalmente sistemas Unix en los servidores de las compañías más importantes, la práctica busca hacer observar al alumno que si bien las contraseñas son cifradas de manera robusta por medio del algoritmo de MD5 en estos sistemas, si éstas resultan simples pueden ser encontradas rápidamente y representar una seria amenaza a la seguridad.

Se eligió el programa “John the Ripper” debido a la robustez con la que cuenta para auditar contraseñas, además de resultar uno de los programas con más opciones para el descifrado. Por otra parte, para complementar el uso de este programa, se utiliza una distribución liveCD de Linux, “<<Back|Track”, que contiene la herramienta usada dentro de su paquetería.

Otro de los motivos por el que se decidió utilizar un liveCD, es que debido a que se afectan directamente archivos del sistema se tiene un riesgo de daños al funcionamiento de las máquinas, por lo que trabajar directamente en los sistemas operativos instalados en el laboratorio representaba un riesgo tanto en la seguridad como en la integridad.

Debido a que “John the Ripper” cuenta con una gran variedad de opciones para auditar contraseñas, la práctica aprovecha esta característica para realizar diversos tipos de ataques a diversas contraseñas. Por consiguiente se realizan los siguientes tipos de pruebas:

- Ataque de fuerza bruta numérico
- Ataque de fuerza bruta alfanumérico
- Ataque de diccionario
- Ataque de fuerza bruta general

Se proponen una serie de contraseñas que se basan en diversas reglas, a fin de determinar qué cambios sencillos como mezclas de minúsculas con mayúsculas, o incursión de números pueden representar una diferencia importante al momento de establecer una contraseña robusta. Por otra parte debido a la potencia del programa, descifrar contraseñas simples resulta bastante rápido, y expone el peligro que representa contar con contraseñas que no siguen reglas básicas de robustez.

5.3.2- Práctica 2 – Firewall (Nivel de Aplicación)

La práctica se enfoca en establecer las diferencias existentes entre diferentes firewalls, y la importancia en que radica tener el más adecuado para las diferentes necesidades de cada uno de los usuarios. Debido a la gran variedad de firewalls existentes en el mercado, se optó por utilizar dos extremos opuestos de enfoque de usuarios, a fin de observar las diversas opciones que existen en el medio.

En primera instancia se utilizó el firewall con licencia de propietario “Zone Alarm” en su versión gratuita, a fin de mostrar un firewall sencillo de uso casero y que puede ser utilizado en situaciones en las cuales ser requiere una protección sencilla para una computadora personal que no contenga información sensible, así como el usuario de dicho equipo no necesite contar con profundos conocimientos de seguridad informática.

El segundo firewall utilizado es “Core Force”, el cual se basa en el filtrado de paquetes creado para el firewall OpenBSD. Debido a esto, la complejidad que encierra es mucho mayor, y requiere que la persona encargada de su configuración y mantenimiento tenga profundos conocimientos de los protocolos de red, así como del funcionamiento de puertos. Este tipo de firewall resultaría más útil en servidores y sistemas dedicados, ya que por defecto, es necesario abrir cada uno de los puertos para que pueda existir comunicación de red.

Para cada uno de los casos, se realizan diversas pruebas de comunicación dentro de la red del laboratorio. Siendo que ambos firewalls trabajan en sistemas Windows, se puede establecer diversos comparativos de funcionamiento, así como establecer en qué situaciones es más conveniente usar cada uno. Por otra parte y debido a la complejidad del firewall “Core Force”, sólo se tratan de manera general los aspectos fundamentales de su funcionamiento, buscando describir sólo los aspectos necesarios para realizar pruebas equivalentes a las realizadas con “Zone Alarm”.

Uno de los aspectos tratados que se intenta destacar, y que usualmente son descuidados en muchos de los casos en que se tiene a cargo un sistema, es la realización de bitácoras que permitan llevar a cabo un registro de actividades y ayuden a determinar una posible amenaza existente. Debido a la complejidad que representan los archivos de registro, se deja como parte de los resultados a entregar el análisis de dichos archivos.

Del mismo modo se da una breve explicación de cómo interpretar cada uno de los archivos de registro, ya que al tratarse de un texto plano resulta complicado entender la información contenida en los mismos si no se cuenta con la experiencia de haber analizado diversos archivos del mismo tipo anteriormente.

Cada uno de los análisis se deja libre para que el alumno de una explicación, ya que los resultados obtenidos no necesariamente tiene que ser los mismos debido a que se registra toda la actividad relacionada a la comunicación dentro de la red con el equipo en cuestión dando como resultado que las variaciones pueden llegar a ser bastante amplias.

Finalmente, para la realización de esta práctica, el alumno debe repasar algunos comandos básicos para la realización de telnet, envió de pings, y conocer los puertos que interactúan para estos casos para la conexión a Internet por medio de un browser.

5.3.3- Práctica 3 – Clientes de Correo Electrónico

La práctica fue originalmente concebida como una sola en conjunto con el cifrado de correo electrónico y firma digital, pero debido a la extensión de la misma se optó por dividirla en dos partes. En esta práctica en particular se pretende instalar un cliente de correo electrónico, analizando algunos conceptos relacionados a protocolos de correo electrónico POP3, IMAP, SMTP.

También se hace uso de métodos enfocados a la transferencia segura de información por medio de los protocolos SSL y TLS. Se tiene cierta flexibilidad en el servidor de correo que se puede usar en el desarrollo de ésta práctica, lo cuál tiene como objetivo que se experimente con diferentes opciones y se observen algunas diferencias en la configuración.

Algunas de las principales características que se pretende sean observadas al usar diversos servidores de correo, es que no todos admiten los protocolos de seguridad SSL y TLS, así como poder compartir diversas experiencias al instalar los clientes de correo usando diferentes proveedores del servicio.

El cliente de correo seleccionado para la realización de esta práctica es “Mozilla Thunderbird”, que cuenta con una amplia variedad de opciones, destacando principalmente la posibilidad de poder instalar diversas extensiones, conocidas como add-ons, y que dicha característica será aprovechada en la siguiente práctica al cifrar el correo electrónico y aplicar una firma digital.

“Thunderbird” cuenta con diversas ventajas sobre otros clientes de correo como es el hecho de tratarse de software libre y ser soportado por diversas plataformas, por lo que si bien en la práctica se propone una instalación en el sistema operativo Windows, la misma práctica puede ser realizada en sistemas operativos Linux sin la necesidad de modificaciones sustanciales al esquema original de la práctica.

El hecho de haber seleccionado Windows para el desarrollo de la práctica obedece principalmente a que se desea mostrar que este tipo de tecnologías pueden ser fácilmente compatibles con sistemas de propietario además de mostrar que existen diversas opciones que pueden ser consideradas al momento de establecer un servicio no sólo de éste tipo, sino cualquier solución que requiera un cliente.

Por otra parte, se incluye el tema del spam, el perjuicio que éste trae consigo y la manera en que afecta diversos medios electrónicos. Del mismo modo, dentro de la práctica en sí, se configura el cliente de correo para establecer políticas sencillas de seguridad que establezcan el bloqueo de dicho tipo de mensajes. Se busca entonces que el alumno generé reglas de filtrado de correo y corroborar el correcto funcionamiento de las mismas.

Otro de los aspectos que se abarca en la práctica, y como parte de la entrega de resultados de la misma, es que el alumno investigue sobre otros programas de clientes de correo electrónico, con la finalidad que conozca otras opciones además de la mostrada en la práctica, y pueda ahondar en otras tecnologías actualmente disponibles.

Un ejemplo de la limitación del Thunderbird en comparación con otros clientes de correo es la falta de de personalización para el manejo de bases de datos, que dependiendo las circunstancias y las necesidades, puede resultar un punto crítico en la elección, por lo que se busca que el alumno visualice este tipo de posibilidades por medio de la investigación planteada.

Como último punto de la práctica, se genera un archivo de respaldo que servirá para la próxima práctica, en el cual se tendrá la configuración del cliente de correo, y sirviendo a su vez a modo de experiencia para generar un respaldo de la información contenida en el programa correspondiente.

5.3.4- Práctica 4 – Firmas Digitales

El objetivo principal de la práctica es poder mostrar a los alumnos la versatilidad e importancia de cifrar mensajes y poder generar firmas digitales. Planeada originalmente en conjunto con la práctica 3, se puede considerar la parte complementaria de la misma ahondando en temas relacionados y sirviendo como base para entender mejor algunas medidas más complejas de control y de seguridad.

Se parte de la primicia de utilizar un algoritmo asimétrico, en el cual se deben tener un par de claves, una pública y una privada siendo la primera la que cualquier usuario puede tener a fin de descifrar los mensajes y corroborar la firma digital y la segunda clave la que utiliza un usuario en particular para cifrar sus mensajes antes de enviarlos a los destinatarios.

Se utiliza para esta práctica, una vez más el cliente de correo “Thunderbird”, con la adición de la extensión “enigmail”, además del programa “GNU Private Guard”, siendo este último la herramienta encargada de cifrar y descifrar los correos. La elección de éste programa se basa en que actualmente es el reemplazo para “PGP”, por lo que se trata de uno de los programas más robustos que existen actualmente además de ser software libre.

En sí, se tienen 2 opciones de algoritmos de cifrado para esta práctica, utilizando ElGamal o bien, RSA. No se especifica ninguno en particular, ya que para fines experimentales y para el alcance de la práctica resulta indistinto elegir uno u otro, sin embargo es conveniente que el profesor en cuestión haga las diferencias pertinentes a cada uno de los algoritmos y explique tanto las ventajas y desventajas de cada uno.

Es importante hacer notar la diferencia que existe entre una firma digital y una firma electrónica, ya que usualmente ambos términos son utilizados indistintamente siendo que ambos tienen diferentes niveles de seguridad y estructura por lo que se trata el tema durante el previo de la práctica.

Para el desarrollo de la práctica es necesario contar con el archivo de respaldo generado durante la práctica pasada, lo cual no necesariamente resulta obligatorio si se ha aprendido cabalmente a configurar una cuenta de correo electrónico con “Thunderbird”, siendo que este proceso puede tomar unos minutos si ya se cuenta con el software instalado y se conocen los pasos a seguir.

Para el cifrado, como se mencionó anteriormente, se utiliza GPG, y debido a que la práctica original fue planteada en el sistema operativo Windows, se utiliza una versión compatible con el mismo: “GPG4win”, con el cual no se interactúa directamente, sino mediante la extensión proporcionada a Thunderbird.

Una de las características más sobresalientes de la práctica es que se requiere una gran interactividad con el grupo, ya que para probar que los mensajes cifrados y que las firmas digitales resultan efectivas, es necesario trabajar en equipo con otros compañeros del laboratorio. Por otra parte, la entrega de resultados exige que se envíe un correo cifrado y firmado al profesor usando la firma digital, lo cual funciona como un indicador de que el alumno ha desarrollado la práctica correctamente.

Finalmente, durante la entrega de resultados se pide una investigación sobre los aspectos legales de la firma digital, siendo que no se específica un país en particular, quedando a consideración del profesor si se desea investigar específicamente en México, o bien destacar las diferencias existentes en diversas partes del mundo.

5.3.5- Práctica 5 – Cómputo Forense (1era Parte)

Esta práctica sirve como una introducción al cómputo forense, utilizando el sistema operativo Linux para su desarrollo. Se hizo así porque dicho sistema cuenta con una gran versatilidad para el análisis de discos, en cualquier sistema operativo, y se busca a su vez reforzar el manejo de la terminal, siendo en ésta ocasión para actividades más complejas que las planteadas en las prácticas iniciales.

En una primera instancia, en el previo se pide que se reafirmen algunos conocimientos con los que el alumno ya debe haber tenido contacto, como lo es el checksum (un algoritmo de suma de verificación en un archivo), o bien qué es un log, o archivos de registros, los cuales fueron tratados en la práctica de firewalls. Posteriormente se pide que se investigue sobre los archivos utmp y wtmp, los cuales son inherentes al sistema Linux y contienen la información de usuarios conectados a un equipo y los ingresos y salidas de usuarios al sistema operativo respectivamente.

Del mismo modo, y debido a que la práctica se origina desde éste punto, se solicita que se investigue información referente a la UNAM-CERT y al reto RedIRIS, a fin de que se profundice en análisis forenses profesionales y se conozcan algunos casos prácticos que han sido mostrados por medio de estas organizaciones, siendo un claro ejemplo los archivos descargados desde los sitios oficiales de dichos organismos y que son utilizados en esta práctica y la siguiente.

La práctica en sí sigue una metodología que si bien puede resultar un poco extensa resulta ser bastante clara. En primera instancia, es necesario utilizar las imágenes de un disco comprometido, el cuál ha sido proporcionado al laboratorio, y que una copia se encuentre dentro de la partición de Linux. Posteriormente se busca guardar una copia de toda la actividad de la terminal en un archivo, a fin de asegurar que el alumno ha trabajado en la práctica.

A continuación se realiza una verificación de las imágenes del disco comprometido por medio de un checksum. Posteriormente se montan las imágenes del disco en el que el orden en que se hiciera resultaría indiferente, pero debido a que se sigue una metodología para trabajar se indica un orden preestablecido.

El siguiente paso marcado es observar diversos archivos, y realizar la copia de dos en particular: “/var/log/messages” y “/.bash_history”, los cuales contienen información sensible que deberá ser analizada posteriormente como parte de los resultados a entregar para esta práctica. Se hace de esta manera, ya que dichos archivos son complejos, y analizarlos requiere cierto tiempo aunque durante la práctica misma se dan puntos esenciales que hay que observar para encaminar al alumno al análisis de este caso en particular.

Existe un archivo que no se pide su análisis durante esta práctica, pero que se hace mención a él, “/var/ftp/nerod” el cual forma parte de un rootkit y que es una parte esencial del estudio del caso. Este archivo es analizado en la siguiente práctica y se decidió de esta manera para evitar que el alumno se vea saturado con la gran cantidad de información manejada a lo largo de la práctica.

Para finalizar las actividades de esta práctica, se pide que las imágenes trabajadas sean desmontadas, aunque en caso de existir algún problema con esto bastaría con reiniciar el sistema operativo para que de manera automáticamente Linux desmonte dichas particiones.

Dentro de los resultados, se pide también la investigación de comandos utilizados comúnmente en cómputo forense, y que algunos de ellos no han sido incluidos dentro de la práctica debido a limitaciones de tiempo como es en el caso del comando “dd”, que realiza copias bit a bit de un disco, y siendo además que dicha tarea puede tomar varias horas.

5.3.6- Práctica 6 – Cómputo Forense (2da Parte)

La segunda parte de la práctica referente al tema de cómputo forense se enfoca en utilizar una herramienta que facilite el análisis forense y permita llevar un registro mas preciso de las actividades realizadas durante el estudio. Por consiguiente, los análisis realizados son los mismos que en la primera parte de la práctica pero de una manera mucho más simple y sencilla esperando que así, sea más comprensible la lógica que se siguió en la parte anterior.

Para la realización de esta práctica se hace uso de la herramienta especializada “Sleuthkit” y el front-end “Autopsy”, ambos incluidos dentro del liveCD <<Back|Track, por lo que se puede optar preferentemente la utilización de dicha distribución para la realización de la práctica aunque es igualmente factible instalar directamente los componentes necesarios en las computadoras del laboratorio dentro del sistema Linux.

Debido a que los conceptos necesarios para esta práctica son bastante similares a los utilizados en la anterior se incluye un previo de repaso. Por consiguiente es necesario que durante la práctica anterior los conceptos planteados hayan sido entendidos claramente ya que en el transcurso de esta práctica se da por hecho que se conocen dichos conceptos y sólo se realiza una ligera revisión de los mismos.

La práctica se basa en que se utilizará el liveCD proporcionado, por lo que inicialmente se indica cómo se debe instalar “Sleuthkit” y posteriormente cómo iniciar “Autopsy”, ya que de manera predeterminada no se encuentran instalados en el sistema. Por otra parte es necesario que una copia de las imágenes de los discos se encuentren ya sea en la unidad de disco duro de la computadora donde se este trabajando, o bien un dispositivo externo como una USB (aunque para éste último caso se requiere de una memoria de gran capacidad, ya que las imágenes resultan ser de un gran tamaño).

En caso de que se opte por tener una copia dentro del disco duro de la computadora, sin importar si se trata de una partición en Windows o en Linux, <<Back|Track monta automáticamente las particiones correspondientes de los sistemas operativos y pueden ser accedidas directamente sin la necesidad del uso de comandos adicionales.

A lo largo de la práctica se observa que se recolecta información referente a las personas que realizan la investigación así como designar un nombre al proyecto y tener registro de la máquina de los posibles casos. Esto se vuelve muy útil al momento de hacer revisiones en los casos por lo que el uso de éstas herramientas tienen la finalidad de guardar un registro de las actividades realizadas por los investigadores.

Con base en lo anterior se busca que los alumnos puedan observar diversas ventajas que se tienen con este tipo de herramientas, ya que una vez que se ha comprendido la metodología básica que debe seguirse para realizar un análisis forense, la práctica busca mostrar cómo es posible ayudarse de herramientas para agilizar las investigaciones.

Si bien, una buena parte de la práctica resulta bastante similar a la anterior, se evita la redundancia de analizar los mismos archivos que la vez pasada, en este caso se analiza otro archivo, “/var/ftp/nerod/install” el cual como se observó anteriormente es parte de un rootkit y muestra cierta complejidad en su análisis. Del mismo modo que en el caso anterior, se da una serie de puntos que el alumno puede seguir para facilitar el análisis.

Finalmente es en esta práctica que se pide como resultado final, que el alumno explique cuál fue la causa que permitió que la máquina fuera comprometida, lo cual resulta fundamental conocer ya que finalmente en todo análisis es necesario

tener un resultado concreto que permita tomar decisiones para prevenir futuros incidentes del mismo tipo.

5.3.7- Práctica 7 – Seguridad en Sistemas y Bases de Datos

La última práctica que se presenta se enfoca en mostrar las posibles vulnerabilidades que pueden ser generadas cuando se crea un sistema en red que hace uso de bases de datos. Para la creación del material utilizado en la práctica se programó un sistema de un gimnasio bastante simple, esto es porque para mostrar los conceptos básicos manejados en la práctica no es necesario tener un sistema con una gran cantidad de módulos.

Por otra parte, el hecho de que el sistema a su vez sea simple es que se utiliza PHP y no es permisible presuponer que los alumnos conozcan el lenguaje a profundidad, estando por demás la utilización de comandos específicos del lenguaje. Por consiguiente en el previo de la práctica se pide una investigación de los comandos que serán utilizados en la práctica a fin de que se entienda la manera en que está creado el sistema.

La elección de PHP es debido a que actualmente es uno de los lenguajes más utilizados en la elaboración de sistemas, por lo que se busca que a la vez los alumnos se interesen tanto en aprender este lenguaje, como buscar comparativos con otras opciones que igualmente existen en el mercado e intentar aplicar los conceptos vistos en otros lenguajes.

Para la realización de la práctica se utiliza un servidor “standalone”, el cual puede ser utilizado de manera individual en una computadora, sin la necesidad de estar conectado a red, además de que presenta gran facilidad para la instalación de los elementos básicos para el funcionamiento de un sistema que son un servidor Apache, una base de datos MySQL y un intérprete de script PHP y Perl. Con base

en esto, se puede enfocar en los conceptos prácticos más que en los técnicos, lo que permite concentrarse en los conceptos que se buscan mostrar en la práctica.

En primera instancia se muestra la instalación del servidor, de manera predeterminada existen varios fallos de seguridad que deben ser corregidos posteriormente como es el caso del establecimiento de contraseñas para la base de datos. Se proporciona al alumno la base de datos que se utilizara, así como las instrucciones para que sea incluida en el sistema.

Posteriormente se dan instrucciones del manejo de “phpMyAdmin”, que es un manejador vía browser de bases de datos en “MySQL”. Se utiliza este manejador ya que viene integrado con XAMPP, además de que no requiere profundos conocimientos de manejo de tablas.

Posteriormente se proporcionan los archivos necesarios del sistema, que vienen incluidos dentro del disco anexo a este documento:

- index.php
- acceso.php
- cursos.php
- inscripciones.php
- secreto.php
- imagenes (carpeta)

Una vez instalado el sistema, se describe de manera breve el funcionamiento, y la manera en que opera. A continuación se describen los siguientes problemas que se presentan en el sistema, y que son corregidos gradualmente:

- Variables visibles para los usuarios – Error o descuido de utilización del método GET por POST.

- Cifrado de información en la base de datos – Aplicación de un comando que cifre la información en la base de datos (evitar de manera cabal el robo de contraseñas).
- Uso de sesiones – Restricción de acceso a ciertas áreas del sistema de manera directa.
- Inyección de código SQL – Validación estricta de los datos ingresados por el usuario.
- Corrección en la configuración de seguridad – Asignación de contraseñas para accesos a bases de datos.

Finalmente, y como parte de profundización en las medidas de seguridad en el desarrollo de sistemas, se pide investigar sobre la abstracción de datos, lo cual resulta de gran utilidad cuando la información manejada resulta ser crítica y es necesario tener medidas extras de seguridad. Del mismo modo se pide una descripción de cómo es que funciona la inyección de código SQL, a fin de que se corrobore que se ha entendido la manera en como este tipo de ataque funciona, y cómo es que deben prevenirse.

5.3.8- Práctica Adicional – Linux Básico

Es una práctica pensada para su realización durante los primeros semestres de la carrera, ya que sirve como una introducción al sistema operativo Linux, abarcando los aspectos más básicos de dicho sistema operativo, ahondando desde la estructura que tienen de manera general para las distintas distribuciones, así como los comandos básicos que se deben conocer para hacer uso de éste desde la línea de comandos.

La práctica no estaba contemplada inicialmente, pero debido a sugerencias dadas dentro de los talleres impartidos a lo largo del desarrollo de las prácticas, se consideró conveniente que los alumnos debieran contar con un nivel de conocimientos mínimos referentes a Linux, por lo que resultaba necesario hacer

una práctica que pudiera servir de introducción, o bien de repaso al manejo de dicho sistema operativo.

Debido a que se trata de una práctica introductoria en sí, no se incluyó un previo que acompañará su desarrollo. Por consiguiente, la mayor parte del aprendizaje de la práctica, se encuentra en el desarrollo mismo de las actividades planteadas. Los comandos que se indican a lo largo del documento, son compatibles con cualquier distribución de Linux, y no es necesario contar con privilegios de administrador para que puedan ser llevados a cabo.

La práctica no representa ningún riesgo para el sistema operativo en que se éste trabajando, en términos que no implica modificación de archivos esenciales para el funcionamiento del mismo. Probablemente para alumnos de los últimos semestres puede resultar bastante sencilla, por lo que no se recomienda su aplicación conjuntamente con el resto de las prácticas, que requieren un grado mayor de conocimientos, sino al inicio de la carrera.

Debido a que se han utilizado comandos que no modifiquen la estructura del sistema operativo en el que se esté trabajando, en los resultados se solicita una investigación sobre comandos que son utilizados para la administración del sistema y que su ejecución implica la instalación de software, creación o eliminación de usuarios, modificación de permisos, etcétera.

Si bien, algunos comandos tienen una breve explicación dentro de la práctica, se deja como tarea al alumno investigar el funcionamiento y la estructura de los mismos, haciendo énfasis en la utilización del comando “man” que es inherente al sistema y en donde se puede encontrar explicación de cada uno de los comandos básicos, con lo que se espera que el alumno pueda posteriormente utilizar el mismo método para entender comandos que utilicé en el futuro.

Durante la práctica se utiliza el editor de texto “nano”, que es bastante común encontrarlo por defecto en la mayoría de las distribuciones Linux, y que resulta bastante sencillo en su utilización. No se ahonda demasiado en él ya que existen diversas opciones que el alumno puede investigar y utilizar posteriormente, como pueden ser los casos de los editores “pico”, “vi” o “emacs”.

Finalmente, esta práctica se plantea de manera adicional como introducción al sistema operativo Linux, aunque se también se propone como un repaso a la utilización desde la línea de comandos de dicho sistema operativo a fin de que en momentos posteriores de la carrera no existan retrasos ocasionados por desconocimiento u olvido de aspectos básicos del sistema.

5.3.9- Anexos

Se incluyen un par de anexos, que sirven como soporte para la realización de las prácticas. El objetivo del Anexo A es explicar de manera general la manera de trabajar dentro del entorno de “<<Back|Track”, principalmente si se requiere trabajar en modo gráfico se explican diversos aspectos de la configuración que deben ser activados para poder trabajar.

Por defecto el sistema no trabaja en modo gráfico por lo que es necesario dar de alta el servicio. Otra característica que se puede resaltar es el hecho de que las memorias USB no se muestran de manera predeterminada en el escritorio del modo gráfico, aunque sí son montadas de manera automática.

El otro anexo, es una serie de direcciones electrónicas donde se puede conseguir todo el material que se utiliza en la práctica, por lo que la finalidad es que el alumno pueda profundizar por su cuenta en el uso de las herramientas utilizadas a lo largo del curso y en cierto modo pueda proporcionar recomendaciones y observaciones que permitan mejorar las prácticas en un futuro.

Conclusiones

El presente trabajo abarca una gran diversidad de temas, que si bien son cubiertos de manera satisfactoria en forma general, existe una gran cantidad de información que no ha podido ser incluida. Para los alcances iniciales que fueron planteados antes de la realización de las prácticas se puede dar por hecho que cumplen con los objetivos trazados.

Si bien resulta imposible abarcar todos los contenidos concernientes a la seguridad informática, siempre es posible marcar una guía que encamine a los alumnos a poder continuar de manera personal con dicho aprendizaje, teniendo en consideración que las prácticas son sólo una plataforma que sirve de soporte para mostrar la base de los temas existentes.

Con base en las observaciones que se obtuvieron de los talleres impartidos, se da por sentado que las prácticas cumplen con las expectativas de fomentar las habilidades necesarias de los estudiantes de la carrera de Ingeniería en Computación y que si bien resultan perfectibles, marcan un precedente para futuras metodologías en la enseñanza de la seguridad en las tecnologías de información.

Es importante destacar que las prácticas tendrán un tiempo de vida relativamente corto ya que debido a los constantes cambios en las tecnologías de la información hacen que la que existe actualmente se vuelva rápidamente obsoleta, por lo que será fundamental realizar cambios periódicos en las herramientas proporcionadas para que lo visto en los laboratorios sea aplicable en el mundo real.

Uno de los aspectos que no es tratado dentro de las prácticas pero que resulta fundamental dentro de la formación de los alumnos es los lineamientos que rigen la ética profesional. Si bien el objetivo fundamental de las herramientas otorgadas es proporcionar los conocimientos necesarios para que los alumnos conozcan

formas de proteger los sistemas, las mismas herramientas pueden ser usadas con fines maliciosos.

Es por tales motivos que recae en el profesor la responsabilidad de establecer claramente los principios éticos que deben regir a los futuros profesionistas, y hacer ver que al igual que en cualquier otra rama de la ciencia, el conocimiento debe ser usado con fines productivos y benéficos para la sociedad ya que finalmente la parte humana tiene un papel de vital importancia en el desarrollo de toda actividad.

Para concluir, se ha podido constatar el hecho de que las herramientas aportadas serán de gran utilidad para los alumnos ya que si bien en cierta medida abordan sólo algunos tópicos elementales de la computación, se puede asegurar que servirán como base en la adquisición de las habilidades primordiales y conocimientos prácticos necesarios para hacer frente a los retos que se presenten a los estudiantes durante el desarrollo de sus futuras actividades profesionales.

Glosario

A

ASCII (American Standard Change for Information integer)
Código de caracteres basado en el alfabeto latino. Utiliza 7 bits para representar los 128 caracteres con los que cuenta, siendo 95 los imprimibles y 33 de control.

ARP (Address Resolution Protocol)
Estándar utilizado a nivel de capa de red para encontrar una dirección de hardware que corresponde a una determinada dirección IP.

B

Blog
Sitio donde las entradas son escritas de manera cronológica, y usualmente contienen información o noticias sobre un tema en particular. La palabra blog es un acrónimo de “web log”.

Bot
Aplicación que corre de manera automática aplicaciones y tareas a través de Internet. También reciben el nombre de “web robots”.

Browser
Aplicación de software que habilita el despliegue de texto, imágenes y otra información multimedia ubicada usualmente en Internet.

C

CC (Criterios Comunes)

Estándar internacional para la seguridad en el cómputo. No proporciona una lista de requerimientos en los productos, sino un marco en el que los usuarios pueden definir sus requerimientos de seguridad.

CERT

El "Centro de Coordinación CERT (CERT/CC)" es el mayor centro de investigaciones enfocadas a los problemas referentes a la seguridad en Internet.

Certificado Digital

Documento digital mediante el que un tercero confiable (una autoridad certificadora), garantiza la identidad de un sujeto y una clave pública.

Cliente de Correo Electrónico

Programa encargado de gestionar el envío y recepción de mensajes de correo electrónico.

Cómputo Forense

Inspección sistemática y tecnológica de los sistemas de cómputo y su contenido a fin de proporcionar evidencia de crímenes informáticos u otros actos que merezcan ser supervisados.

Criptografía

Rama de las matemáticas que hace uso de métodos y técnicas que tienen por finalidad el cifrar datos o información a través de algoritmos haciendo uso de claves.

Criptosistema

Conjunto de procedimientos y algoritmos que participan dentro de la criptografía.

Criptoanálisis
Códigos y algoritmos empleados para romper el cifrado de la información, es una ciencia complementaria de la criptografía.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
Protocolo de control el cual tiene por principal función es mejorar el desempeño de las redes por medio de la detección de colisiones asignando tiempos de espera para la retransmisión de la señal.

Checkpoint
Punto de referencia de información utilizada por la computadora durante la transmisión de datos.

Checksum
Medida de control para proteger la integridad de la información, la cual verifica que los datos no hayan sido corrompidos.

D

Diccionario, ataque
Técnica para romper el mecanismo de autenticación en un sistema, el cual consiste en probar una gran diversidad de claves y contraseñas incluidas en un archivo con una lista de palabras.

Dialer
Programa que crea una conexión a Internet u otro tipo de de red de manera automática a través de una línea telefónica o bien utilizando un protocolo PPP (punto a punto).

DNS (Domain Name System)

Base de datos que almacena información asociada a nombres de dominios y redes. Es usada en Internet para asociar nombres de dominios con direcciones IP.

DoS (Denial of Service)

Ataque dirigido a un sistema de cómputo o a una red y cuyo objetivo se centra en provocar que los recursos y servicios sean inaccesibles para los usuarios legítimos.

E

ElGamal

Algoritmo de criptografía asimétrica, usado en PGP y GnuPG. Para generar un par de claves, se escoge un número primo n y dos números aleatorios p y x menores que n, calculándose entonces: $y = p^x mod n$. La clave publica es (p, y, n), mientras que la clave privada es x. Escogiendo n primo, garantizamos que sea cual sea el valor de p, el conjunto {p, p2, p3 . . .} es una permutación del conjunto {1, 2,..., n − 1}.

Ethernet

Tecnología utilizada por redes de computadoras de área local que utiliza tramas de datos. Ethernet define las características del cableado a nivel físico y los formatos de las tramas a nivel de enlace del modelo OSI.

Exploits

Programas maliciosos, fragmentos de código o una secuencia de comandos que buscan aprovechar o tomar ventaja de algún error o vulnerabilidad en el software a fin de ocasionar cierto comportamiento inesperado en el sistema.

F

Flood, ataque

Ataque de denegación de servicio (DoS) a los sistemas de computación en el cuál el objetivo es saturar a la víctima con peticiones de respuesta de conexión.

Firewall

Elemento de software o hardware utilizado para establecer un control de acceso a una red de computadoras, previniendo comunicaciones no permitidas por las políticas de seguridad.

Firma Digital

Secuencia de bits que son añadidos a una pieza de información cualquiera y que permite garantizar su autenticidad sin depender del proceso de transmisión. Se utilizan algoritmos asimétricos y forma parte de un subconjunto de la firma electrónica.

Firma Electrónica

Sonido, símbolo o proceso electrónico unido o asociado inherentemente a un recurso y el cuál es ejecutado o adoptado por una persona a fin de poder “firmar” dicho recurso.

FTP (File Transfer Protocol)

Protocolo establecido en la capa de aplicación y cuyo principal objetivo es la transferencia de archivos entre sistemas conectados mediante una red y el cual se basa en una arquitectura cliente-servidor.

Fuerza bruta, ataque

Técnica en el que se busca obtener una clave o contraseña probando todas las combinaciones posibles hasta encontrar aquella que permita el acceso a un determinado sistema.

Full Duplex, transmisión
Sistema de comunicación bidireccional en el que los canales de comunicación transmiten y reciben información de manera simultánea.

G

GnuPG (GNU Privacy Guard)
Software libre reemplazo de PGP utilizado para cifrado de mensajes y manejo de firmas digitales.

H

Hacker
Persona con altos conocimientos de cómputo, quien se enfoca principalmente en los mecanismos de seguridad de los sistemas informáticos.

Half Duplex, transmisión
Sistema de comunicación bidireccional en el que los canales de comunicación transmites y reciben información de manera no simultánea.

HAM
Nombre empleado por la organización Askimet para diferenciar mensajes legítimos del spam en los blogs.

Hash
Resultado de aplicar una función o método para generar claves que representen de manera unívoca a un documento o archivo.

HTTP (Hyper Text Transfer Protocol)
Protocolo utilizado para la gestión de páginas web. Es el sistema por medio del cuál se envían peticiones de acceso y respuestas de contenido.

I

ICMP (Internet Control Message Protocol)
Protocolo de diagnostico y notificación de errores en Internet. Generalmente no interactúa directamente con las aplicaciones finales del usuario, con las excepciones de las herramientas “ping” y “traceroute”.

IMAP (Internet Message Access Protocol)
Protocolo para acceso de mensajes electrónicos almacenados en un servidor. Mediante este protocolo se tiene acceso al correo electrónico.

INFOSEC (Information Security)
Proceso de protección de datos contra acceso, uso, modificaciones, eliminación, corrupción o redistribución no autorizado. Las principales metas son proteger la integridad, la confidencialidad y la disponibilidad de la información.

Ingeniería Social
Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

Insider
Miembro de un grupo cualquiera con acceso a un área restringida. El concepto se utiliza en el contexto de la información.

Inyección de código

Técnica que aprovecha la vulnerabilidad derivada de una incorrecta validación de los datos recibidos por un usuario al sistema, a fin de poder ganar accesos restringidos en una determinada base de datos.

IP (Internet Protocol)
Protocolo no orientado a la conexión, usado tanto por el origen como por el destinatario para la comunicación de datos a través de una red de paquetes conmutados.

IRC (Internet Relay Chat)
Protocolo de comunicación en tiempo real basado en texto que permite charlas entre dos o más personas.

IT (Information Technology)
Se refiere al estudio, diseño, desarrollo, implementación, mantenimiento y manejo de sistemas de información basados en la computación particularmente en aplicaciones de software y hardware de computadora.

ITU-T (ITU Telecomunication Standarization Sector)
Comité encargado de la normalización de las telecomunicaciones.

K

Keylogger
Herramienta de software utilizada para registrar en un archivo las pulsaciones que se realizan sobre el teclado.

L

LiveCD
Sistema operativo, generalmente acompañado con un conjunto de aplicaciones, que es almacenado en un medio extraíble como un CD o DVD.

Linux
Sistema operativo tipo Unix que es uno de los paradigmas más prominentes del software libre. También se le conoce con éste nombre al núcleo del mismo sistema.

Log
Archivo generado de manera automática por un programa dedicado a registrar eventos específicos en un sistema.

M

Malware
Software diseñado para infiltrarse en un sistema de computación sin el conocimiento del usuario con la finalidad de causar algún tipo de daño a dicho sistema.

MD5 (Message-Digest Algorithm 5)
Algoritmo criptográfico de reducción de 128 bits utilizado para obtener funciones hash.

O

Open Source
Término con el que se designa al software distribuido y desarrollado libremente.

OSI, modelo (Open Systems Interconnection Basic Reference Model)
Modelo abstracto y en capas que describe las comunicaciones en red y el diseño de protocolos de conexión entre computadoras.

Outsourcing
Término referido para indicar cuando una empresa destina recursos orientados para la realización de una tarea a una empresa externa por medio de un contrato.

P

Ping
Utilidad que comprueba el estado de una conexión con uno o varios equipos remotos por medio de respuestas de eco.

PGP (Pretty Good Privacy)
Programa utilizado para proteger información distribuida a través de Internet por medio del uso de criptografía así como permitir la autenticación de documentos por medio de una clave pública.

POP3 (Post Office Protocol)
Protocolo utilizado para descargar en un cliente local los mensajes de correo electrónico almacenados en un servidor remoto.

Pop-up

Medio de publicidad en Internet que tiene por finalidad incrementar el tráfico a un sitio web o capturar direcciones de correo electrónico.

R

Rootkit

Grupo de herramientas de software usadas para esconder procesos y archivos que permitan a un usuario no legítimo tener acceso a un sistema. De manera justificada se utilizan en la auditoria de los sistemas informáticos.

Router

Dispositivo de hardware utilizado para la interconexión de redes de computadora. El router es el encargado de encaminar los datos a través de las diferentes redes.

RSA

Algoritmo asimétrico cifrador de bloques que utiliza un par de claves, una pública y una privada, que fue desarrollado en 1978 por Ron Rivest, Adi Shamir y Leonard Adleman.

S

Script

Programa que generalmente se almacena en un archivo de texto plano, y es típicamente escrito en lenguaje interpretado

Servidor de correo

Agente de transporte de correo, encargado de gestionar los e-mails. El usuario final no tiene acceso directo al servidor de correo.

Software Libre

Software que puede ser usado, copiado, estudiado modificado y redistribuido libremente. No se debe confundir con el término software gratuito, el cuál no tiene costo pero no puede ser redistribuido ni modificado.

Spam

Envío de mensajes de manera masiva a diversos destinatarios cuyo contenido es en su gran mayoría de tipo publicitario y los cuales resultan indeseados para los usuarios

SSH (Secure Shell)

Protocolo de red que permite el intercambio de datos sobre un canal seguro entre dos computadoras.

SSL (Secure Socket Layer)

Protocolo criptográfico que provee comunicación segura en diversas interfases, como browsers, mensajería instantánea, correo electrónico y diversos tipos de transferencia de datos.

SMTP (Simple Mail Transfer Protocol)

Protocolo basado en texto que es el estándar para la transmisión de correo electrónico en Internet.

Smurf, ataque

Ataque de denegación de servicios (DoS) que utiliza mensajes ping dirigidos al broadcast para saturar la comunicación en un sistema.

Spoofing, ataque

Ataque informático que consiste en que un atacante, ya sea una persona o un programa, falsifique su identidad haciéndose pasar por otro usuario o equipo legítimo ganado acceso a recursos restringidos del sistema.

Spyware

Aplicación que recompila información referente al usuario de un equipo sin el consentimiento del mismo.

SQL (Structured Query Language)

Lenguaje de computadora utilizado para el manejo y recuperación de información en un sistema administrador de bases de datos relacionales.

Standalone, servidor

Compilación de programas que se ejecutan en una computadora personal y que emulan el comportamiento del mismo grupo de programas funcionando en un servidor en Internet.

Switch

Dispositivo electrónico de interconexión de redes de computadora que opera en la capa 2 del modelo OSI:

T

TCP (Transmission Control Protocol)

Uno de los protocolos fundamentales de Internet encargado de la transmisión de paquetes de datos y de distinguir diversas aplicaciones que hacen uso de las redes por medio del concepto de puertos.

TLS (Transport Layer Security)

Protocolo para la transmisión segura de la información en Internet. Es el sucesor del protocolo SSL.

Telnet (Teletype Network)
Protocolo utilizado para manipular una máquina a través de una conexión de red de manera remota.

Trashing
Práctica referente a la obtención de información por medio de la inspección de la basura de un usuario, esperando encontrar información sensible contenida dentro de la misma.

U

Unix
Familia de sistemas operativos multitarea, multiusuarios y portables, que comparten ciertos criterios de diseño e interoperatibilidad.

UDP (User Datagram Protocol)
Protocolo que permite el envió de datagramas a través de la red sin la necesidad de haberse solicitado previamente una conexión.

US-CERT (United States Computer Emergency Readiness Team)
Organización que forma parte de la “National Cyber Security Divison” del “Departamento de Seguridad Nacional de los Estados Unidos”.

V

Virus

Programa de computadora que se copia a si mismo teniendo como objetivo causar alteraciones en el funcionamiento normal de un sistema sin el consentimiento del usuario.

W

Windows

Sistema operativo con interfaz gráfica cuyo propietario es la empresa Microsoft.

Bibliografía

BAJULA García Walter, "*Los Ataques Spoofing. Estrategia General Para Combatirlos*", Febrero 2002 [ref. del 14 de marzo del 2007], Disponible en Web: <http://www.virusprot.com/Art23.html>

CANELADA Oset Juan Manuel, "Análisis Forense de Sistemas Linux", Universidad Autónoma de Madrid, 2004, [ref. del 28 de Enero del 2007], Disponible en Web: <http://crl.iic.uam.es/descargas_web/cursos_verano/20040801/JuanMa_Canelada/Analisis_forense_de_sistemas.pdf >

HORTON Mike; MUGGE Clinton, "*Claves Hackers"*, Ed. Mc Graw Hill / Interamericana de España, 2004

LÖPEZ Barrientos María Jaquelina, QUEZADA Reyes Cintia, "Fundamentos de Seguridad Informática" Universidad Nacional Autónoma de México, México

LUCENA López Manuel J. "Criptografía y Seguridad en Computadores", 4ª Edición, Versión 0.7.5, [ref. del 31 de marzo del 2007], Disponible en Web: <http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto/>

PIEPRZYK Josef, HARDJONO Thomas, SEBERRY Jenifer, "Fundamentals of Computer Security", Ed. Springer-Verlang, Alemania, 2003

RAMIÓ Aguirre Jorge, "Libro Electrónico de Seguridad Informática y Criptografía", Universidad Politécnica de Madrid, España, 2006, [ref. del 6 de Abril del 2007]. Disponible en Web: <http://www.criptored.upm.es/guiateoria/gt_m001a.htm>

SÁNCHEZ Prieto Sebastián, GARCÍA Poblacion Oscar, "Unix y Linux, Guía Práctica", Ed. Alfaomega, 3ea Edición, España, 2005

SCAMBRAY Joel; SHEMA Mike, "*Hackers de Sitios Web: Secretos y Soluciones para la seguridad de los sitios Web*", Ed. Mc Graw Hill / Interamericana de España, 2003.

TEJERO Gómez Luis Gerardo, "Cómputo Forense", Facultad de Ingeniería, UNAM, México, 2006

VILLALÓN Huerta Antonio, "*Seguridad en Unix y Redes*", Julio 2002 [ref. del 26 de enero del 2007], Disponible en Web: <http://www.virusprot.com/Art23.html>

ZIEGLER Robert L., traducción: SÁNCHEZ José Ignacio, "Guía Avanzada Firewalls Linux", Ed. Prentice Hall, España, 2000

Mesografía

"Linux Users 7", MP Ediciones, Argentina [ref. del 22 de Noviembre del 2007], Disponible en Web: <http://www.tectimes.com/magazines/linux/lnx007/>

"Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006", Trusted Strategies, 2006, [ref. del 22 de Noviembre del 2007], Disponible en Web: <https://forms.phoenix.com/cybercrime/docs/cyberdoc.pdf>

Asociación de usuarios GNU / Linux en Cantabria, [ref. del 20 de Junio del 2007], <http://linuca.org>

Boletines publicados por DGSCA, [ref. del 3 de Abril del 2007], <http://biblioteca.dgsca.unam.mx/cu/productos/boletines>

Centro de Investigación Argentina, [ref. del 12 de Febrero del 2007], <http://www.cisiar.org/>

Clasificación de certificados digitales de acuerdo a Verisign, [ref. del 20 de Febrero del 2007], <http://www.verisign.com/repository/hierarchy/hierarchy.pdf>

Informe del impacto del malware en la economía por parte de Computer Economics, [ref. del 10 de Junio del 2007], <http://www.computereconomics.com/>

Estadísticas Askimet, [ref. del 14 de marzo del 2007], <http://akismet.com/stats/>

Estadísticas CERT/CC, [ref. del 10 de Noviembre de 2006], <http://www.cert.org/stats/>

Estadísticas Netcraft, [ref. del 25 de Febrero del 2007], <http://survey.netcraft.com/surveys/analysis/https/2005/Jun/>

Estudio de percepción en seguridad informática en México de Joint Future Systems, S.C. [ref. del 20 de Julio del 2007], <http://www.jfs.com.mx/e2007.htm>

Free Software Foundation Europa, [ref. del 10 de Junio del 2007], <http://fsfeurope.org>

Información proporcionada por Symantec, [ref. del 14 de Noviembre del 2006], <http://www.symantec.com/region/mx/enterprisesecurity/content/expert/>

Portal de Seguridad Informática, [ref. del 25 de Junio del 2007], <http://www.net-security.org>

Recomendaciones Stopbadware.org, [ref. del 20 de Enero de 2007], <http://stopbadware.org/home/security>

United States Computer Emergency Readiness Team (US-CERT), [ref. del 22 de Noviembre del 2006], <http://www.us-cert.gov>