UNIVERSIDAD AUTONOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM TEXCOCO

ESTRATEGIAS DE SEGURIDAD LOGICA

TESIS

QUE PARA OBTENER EL GRADO DE

LICENCIADO EN INFORMATICA ADMINISTRATIVA

P R E S E N T A N:

BLANCAS MARTÍNEZ JOSÉ DE JESÚS
FRANCO AYALA ALFREDO

ASESOR:

MAT. GÓMEZ AYALA HIPÓLITO

REVISORES:

LIC. MARTINEZ AVIDA ANA LUISA
ING. ROBLES GIL FERNANDO
LIC. QUINTOS RAMIREZ ANGEL RAFAEL

Texcoco, México **Julio 2010**

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

INTRODUCCIÓN

El gran uso de las computadoras y redes como medios de almacenamiento, transferencia y procesamiento de información se ha incrementado, al grado de convertirse en un elemento indispensable para el funcionamiento de diversas organizaciones (escuelas, empresas, centros de cómputo, hogares entre otros). Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de gran valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad, disponibilidad, e integridad.

La inseguridad en la manipulación de la información, es cada día más vulnerable, por ejemplo un caso reciente fue la denuncia de un miembro del equipo de Obama (presidente electo de los estados unidos nov. 2008), quien denunció al Servicio Secreto de EE UU y al FBI un problema con un ordenador, que él imputaba a un virus informático. Sin embargo, cuando los agentes revisaron el sistema concluyeron que “una gran cantidad de información fue extraída de sus computadoras".

El FBI aseguró al equipo de Obama que no habían sido las únicas victimas, el sistema de campaña de su rival, John McCain, también había sido quebrantado. Según publica la revista Newsweek, que ha descubierto el caso, las investigaciones apuntan a una "entidad u organización extranjera" que quisiera reunir información confidencial de cara a una futura negociación con el nuevo presidente.

Casos como este originan que diferentes organizaciones busquen mecanismos cada vez más seguros, retomando el ejemplo anterior esto se puede evitar contando con estrategias idóneas hacia la seguridad, puesto que el daño que tuvieron fue irreversible.

Es importante mencionar que un esquema de seguridad contempla la seguridad física y lógica de una compañía. La primera se refiere a la protección contra robo o daño al personal, equipo e instalaciones de la empresa; y la segunda está relacionada con el tema que nos ocupa: la protección a la información, a través de una arquitectura de seguridad eficiente, además se refiere a la seguridad de información comúnmente como la protección de sistemas de información contra el acceso no autorizado o la modificación de información, si está en una fase de almacenamiento, procesamiento o tránsito. También la protege contra la negación y provisión de servicios a usuarios no autorizados, incluyendo las medidas necesarias para detectar, documentar, y contrariar tales amenazas.

Esta última debe ser proactiva, integrar una serie de iniciativas para actuar en forma rápida y eficaz ante incidentes y recuperación de información, así como elementos para generar una cultura de seguridad dentro de la organización.

PLANTEAMIENTO DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

Resultan muy importantes las estrategias de seguridad informática por la existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red para modificar, sustraer o borrar datos.

Estos personajes pueden formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más del 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su organización. Así mismo existe la alteración de la información por falta de conocimiento de las medidas de seguridad disponibles por personal de la organización (cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan).

El internet ofrece un mundo de posibilidades de acceso a la información y servicios tales como web[1], ftp[2], email, bibliotecas con grandes bases de datos de todo tipo de información como académica, científica, comercial, entre muchos otros servicios.

Desde que se consolido Internet como medio de interconexión y comunicación mundial, los incidentes de seguridad relacionados con los sistemas informáticos vienen incrementándose de manera constante. Casos como estos vienen provocando una creciente necesidad de establecer mecanismos de protección que reduzcan al mínimo los riesgos asociados al robo de información.

[1] Web: Mecanismo proveedor de información electrónica para usuarios conectados a Internet.

[2] ftp: Acrónimo de *File Transfer Protocol,* protocolo de transferencia de archivos que se utiliza en Internet y otras redes para transmitir archivos entre servidores o entre un usuario y un servidor.

Es por ello que asegurar la información se convierte en una necesidad dentro de cualquier institución u organización, en la actualidad existen diversas formas de pérdida de información ya sea por ataques de virus informáticos, sabotaje de terceros, o hackers[3].

Estas situaciones se presentan debido a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las organizaciones, el resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos de la organización, lo que representa un daño con valor incalculable.

Causas de ello es que no existe conocimiento relacionado con la planeación e implementación de estrategias de seguridad eficientes que proteja toda su información.

[3] Hacker: estos últimos también conocidos como piratas informáticos que buscan tener acceso a la red para modificar, sustraer o borrar datos.

JUSTIFICACION

JUSTIFICACIÓN

En un sistema informático los elementos a considerar para su protección son el hardware, el software y los datos. El hardware son todos los elementos físicos de un sistema informático, como CPU, terminales, cableado, monitor, teclado o medios de almacenamiento. El software es el conjunto de programas lógicos que hacen funcional el hardware, tanto sistemas operativos como aplicaciones, y los datos que es aquella información lógica.[4]

Los datos constituyen el principal elemento a proteger, es el más amenazado y el más difícil de recuperar, por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren, estas técnicas las brinda la seguridad lógica.

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos, así sólo permitir acceder a ellos a las personas autorizadas para hacerlo. Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Para ello, resulta importante establecer estrategias de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos, hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

Diseñar e implantar estrategias de seguridad lógica evitan la violación de los sistemas, pérdida o modificación de los datos de la organización, lo que puede representar una excelente operación con toda la información que maneja.

[4] Información lógica: Son los paquetes que circulan por un cable de red o entradas de una base de datos.

OBJETIVOS

OBJETIVO GENERAL

Proponer estrategias de seguridad lógica, mediante el análisis de los recursos comunes de las organizaciones, para garantizar que los recursos informáticos estén disponibles y cumplir con los propósitos para los que fueron creados.

OBJETIVOS PARTICULARES

- Analizar las principales amenazas y mecanismos de inseguridad asociados al acceso y transmisión de la información en los sistemas informáticos.
- Elaborar las estrategias de seguridad lógica que se adapten a las organizaciones acorde a sus necesidades, asegurando que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Elaborar los lineamientos para la implementación de las estrategias de seguridad lógica que se adoptaran para garantizar la seguridad de los datos.

SUPUESTO

Al implementar una estrategia de seguridad lógica, se disminuirán las anomalías dentro de una organización.

CAPITULO I

SEGURIDAD INFORMATICA

CAPITULO 1 SEGURIDAD INFORMATICA

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

La mayor parte del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesarios para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el conocimiento con que se cuenta.

Es por ello que la seguridad informática nos permite asegurar que los recursos del sistema de información[5] de una organización sean utilizados de la manera que se decidió y el acceso a la información, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de autorización.

La seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones[6] y dispositivos.

En una definición más completa, Álvaro Gómez Vieites define a la seguridad informática como “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confiabilidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios no autorizados al sistema.

[5] Es un conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones.
[6] Programa informático que permite a un usuario utilizar una computadora con un fin especifico.

La seguridad informática se divide en dos vertientes:

La primera es la seguridad física, que hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático para proteger el hardware de amenazas físicas.

Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza. Básicamente las amenazas físicas que pueden poner en riesgo un sistema de información son:

- Desastres naturales, incendios, humedad e inundaciones
- Amenazas ocasionadas involuntariamente por personas
- Acciones hostiles deliberadas como robo, fraude o sabotaje

La segunda es la seguridad lógica, que es la configuración adecuada de un sistema para evitar el acceso a los recursos y configuraciones del mismo por parte de personas no autorizadas, así mismo hace referencia a las aplicaciones de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático.

Para el presente, abordaremos la seguridad lógica, ya que un sistema de información ciento por ciento seguro es casi imposible, pero con buenas medidas o estrategias de seguridad lógica se podrán evitan daños y problemas.

La seguridad lógica de un sistema informático se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una computadora y controlar el mal uso de la información; aplicando los procedimientos que aseguren que solo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo, el uso de software, la protección de los datos, proceso y programas, así como la del acceso ordenado y autorizado de los usuarios de la información.

1.1 CONCEPTO DE SEGURIDAD LOGICA

La seguridad lógica se entiende como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial, en este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales[7].

La seguridad lógica de un sistema informático incluye:

- Restringir al acceso a programas y archivos mediante claves y/o encriptación.
- Asignar las limitaciones correspondientes a cada usuario del sistema informático.
- Esto significa, no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo.
- Asegurarse que los archivos y programas que se emplean son los correctos y se usan correctamente. Por ejemplo, el mal uso de una aplicación puede ocasionar agujeros en la seguridad de un sistema informático.
- Control de los flujos de entrada/salida de la información. Esto incluye que una determinada información llegue solamente al destino que se espera que llegue, y que la información llegue tal cual se envió.

El objetivo de la seguridad lógica es mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora.[8]

Con el pasar de los años, las computadoras pasaron de ser grandes monstruos, que ocupaban salas enteras, a pequeños elementos de trabajos perfectamente ubicables sobre un escritorio de oficina. En este proceso de digitalización y miniaturización llamado "downsizing" la característica más importante que se perdió fue la seguridad.

[7] http://www.cuentame.inegi.gob.mx/museo/cerquita/redes/seguridad/intro.htm
[8] ALDEGANI, Gustavo. Miguel. Seguridad Informatica.MP Ediciones. 1997. Página 22

1.1.1 ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD LOGICA

Para comenzar el análisis de la seguridad lógica se deberá conocer las características de lo que se pretende proteger: la Información.

Así, definimos dato como la unidad mínima con la que compone cierta información[9].

La información es una agregación de datos que tiene un significado específico más allá de cada uno de éstos[8], y tendrá un sentido particular según como y quien la procese.

Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es información.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la información:

1. Es Crítica: Es indispensable para garantizar la continuidad operativa.
2. Es Valiosa: Es un activo con valor en sí misma.
3. Es Sensitiva: Debe ser conocida por las personas que la procesan y sólo por ellas.

[9] CALVO, Rafael Fernández. Glosario Básico Ingles - Español para usuarios de Internet. 1994-2000.http://www.ati.es/novatica/2000/145

La integridad de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La disponibilidad u operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La privacidad o confidencialidad de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño. El control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades. Pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica:** Mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- **No Repudio:** Mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- **Consistencia:** Se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** Este aspecto, íntimamente relacionado con la **Confidencialidad**, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoria:** Es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.
- Cabe definir **Amenaza**, en el entorno informático, como cualquier elemento que comprometa al sistema (figura 1.1)

Figura 1.1 - Amenazas para la Seguridad
HUERTA, Antonio Villalón. Seguridad en Unix y Redes

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. **La Prevención (antes):** Mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
b. **La Detección (durante):** Mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
c. **La Recuperación (después):** Mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo[10] debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

El daño es el resultado de la amenaza; aunque esto es sólo la mitad del problema. El daño también es el resultado de la no-acción, o acción defectuosa, del administrador del sistema. El daño puede producirse porque el administrador de sistema no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad.

El protector será el encargado de detectar cada una de las vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las contramedidas (técnicas de protección) adecuadas.

Según algunos especialistas la seguridad es muy difícil de conseguir en un 100% por lo que sólo se habla de fiabilidad y se la define como la probabilidad de que un sistema se comporte tal y como se espera de él[11], y se habla de sistema fiable en lugar de sistema seguro.

Para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad.

---

[10] La proximidad o posibilidad de un daño sobre un bien. CALVO, Rafael Fernández. Glosario Básico Ingles - español para usuarios de Internet. 1994-2000.http://www.ati.es/novatica/2000/145

[11] HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital. http://www.kriptopolis.com

Se deberá conocer "qué es lo que queremos proteger", "de quién lo queremos proteger", "cómo se puede lograr esto legislativa y técnicamente"; para luego concluir con la formulación de estrategias adecuadas de seguridad.

1.1.2 IMPORTANCIA DEL SISTEMA DE SEGURIDAD

En algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. "Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar.

Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

Las distintas funciones que se deben asegurar en un sistema informático y los principales puntos que se deben tomar en cuenta en un sistema de seguridad son[12]:

1. **Reconocimiento**: Cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.
2. **Integridad**: Un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.
3. **Aislamiento**: Los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento). También se debe lograr independencia entre los datos accesibles y los considerados críticos.
4. **Auditabilidad**: Procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema.

Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:

- ¿El uso del sistema es adecuado?
- ¿El sistema se ajusta a las normas internas y externas vigentes?
- ¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?
- ¿Todas las transacciones realizadas por el sistema pueden ser registradas adecuadamente?
- ¿Contienen información referente al entorno: tiempo, lugar, autoridad, recurso, empleado?

[12] HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital. http://www.kriptopolis.com

5. **Controlabilidad:** Todos los sistemas y subsistemas deben estar bajo control permanente.
6. **Recuperabilidad**: En caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.
7. **Administración y Custodia:** La vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

1.1.3 DE QUIEN DEBEMOS PROTEGERNOS

Se llama intruso o atacante a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita[13] menciona lo siguiente:

Los tipos de Intrusos podemos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide (figura 1.2):

1. **Clase A:** El 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, son pequeños grupitos que se juntan y dicen vamos a probar.
2. **Clase B:** Es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.
3. **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

[13] ARDITA, Julio Cesar. Director de Cybsec S.A. Security Sistem y ExHacker. Http://cybsec.com

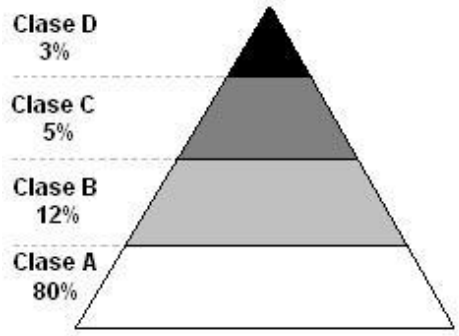

Figura 1.2 – Tipos de Intrusos.
Cybsec S.A. http://www.cybsec.com

1.1.4 QUÉ DEBEMOS PROTEGER

Los datos que maneja un sistema son los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y aún así es difícil de devolver los datos a su forma anterior al daño.

Existen multitud de amenazas y ataques que se los puede clasificar en:

1. **Ataques Pasivos**: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son interceptar los datos y el análisis de tráfico (figura 1.3). Generalmente se emplean para:

- Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

- Es posible evitar el éxito, si bien no el ataque, mediante el cifrado de la información y otros mecanismos que se verán posteriormente.

2. **Ataques Activos**: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

- Interrupción: Si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- Intercepción: Si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- Modificación: Si además de conseguir el acceso consigue modificar el objeto.
- Fabricación: se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
- Destrucción: es una modificación que inutiliza el objeto.

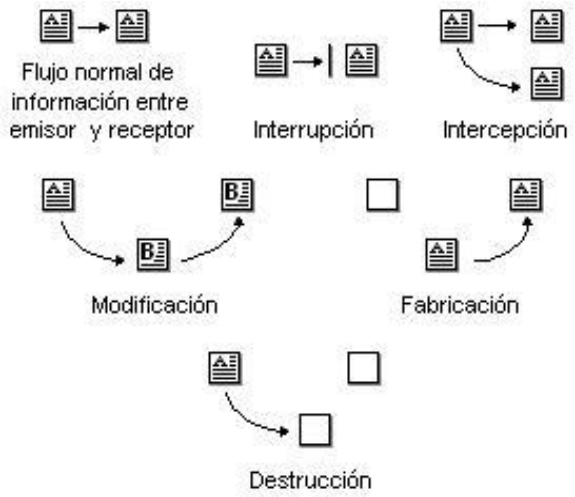

Figura 1.3 - Tipos de Ataques Activos.
http://www.cert.org.mx

Con demasiada frecuencia se cree que los piratas son lo únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

CAPITULO II

AMENAZAS HUMANAS

CAPITULO II AMENAZAS HUMANAS

Las organizaciones cada vez son más dependientes de la tecnología informática, sin un sistema informático los procesos de cualquier organización no funcionarían.

Tenemos grande redes, Internet, diversidad de plataformas, múltiples sistemas operativos, usuarios internos, externos e invitados, equipos móviles, etc., que hacen que la información viajen de un lugar a otro, expuesta a amenazas latentes, esperando atacar.

En este capítulo definiremos las amenazas humanas que pueden atentar contra la seguridad lógica de una organización. Es importante analizar cada unos de los individuos para poder tomar medidas y emplear estrategias en la seguridad.

2.1 DEFINICIÓN DE HACKER

Un hacker es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (Free Information), distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.
- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el hackers sino el Cracker[14].

[14] Crack (en ingles) Grieta. La traducción del término Cracker al es pañol es “el que produce una grieta”

Pero entonces veamos que **sí** es un **Hacker**[15]:

1. Un verdadero Hacker es curioso y paciente. Si no fuera así terminarían por hartarse en el intento de entrar en el mismo sistema una y otra vez, abandonando el objetivo.
2. Un verdadero Hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conocen y que les aburre. ¿Por qué destruir algo y perderse el placer de decir a los demás que hemos estado en un lugar donde ellos no han estado?
3. Un Hacker es inconformista, ¿porqué pagar por una conexión que actualmente cuesta mucho dinero, y además es limitada? ¿Porqué pagar por una información que solo van a utilizar una vez?
4. Un Hacker es discreto, es decir que cuando entra en un sistema es para su propia satisfacción, no van por ahí cantándolo a los cuatro vientos. La mayoría de los casos de "Hackers" escuchados son en realidad "Fantasming". Esto quiere decir, que si un amigo se entera que se ha entrado en cierto sistema; "el ruido de los canales de comunicación" hará que se termine sabiendo que se ha entrado en un sistema cinco veces mayor, que había destruido miles de ficheros y que había inutilizado el sistema.
5. Un Hacker disfruta con la exploración de los detalles de los sistemas programables y aprovecha sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible.
6. Un Hacker programa de forma entusiasta (incluso obsesiva), rápido y bien.
7. Un Hacker es experto en un programa en particular, o realiza trabajos frecuentemente usando cierto programa. Por ejemplo programador en C.
8. Los Hackers suelen congregarse. Tiende a connotar participación como miembro en la comunidad global definida como "La red".

[15] Definición extraída y traducida de http://murrow.journalism.wisc.edu/jargon/jargon.html

9. Un Hacker disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.
10. Antiguamente en esta lista se incluía: Persona maliciosa que intenta descubrir información sensible: contraseñas, acceso a redes, etc. Pero para este caso en particular los verdaderos Hackers han optado por el término Cracker.

Los hackers cambian precisamente la fabricación de la información en la que se sustenta la sociedad y contribuyen al flujo de tecnología. En el peor, los Hackers pueden ser traviesos perversos o exploradores curiosos. Los Hackers no escriben dañinos virus de computadora. Los virus dañinos están completamente en contra de la ética de los Hackers[16].

2.2 CRACKERS

Los crackers, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la manera equivocada o simplemente personas que hacen daño solo por diversión.

2.3 PHREAKERS

El phreaking[17], es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que lo Phreakers son Cracker de las redes de comunicación. Personas con amplios (a veces mayor que el de los mismo empleados de las compañías telefónicas) conocimientos en telefonía, tal es el caso de Kevin David Mitnick quien en 1995 entro al sistema de Motorola para poder realizar las llamadas sin que tuvieran algún costo.

[16] Texto extraído y traducido de http://www2.vo.lu/homepages/phahn/humor/hacker30.txt
[17] Fusión de las palabras Freak, Phone y Free: Monstruo de los Teléfonos Libres (intento de traducción literal)

2.4 CARDING - TRASHING

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabajaba para conseguir una tarjeta de crédito ajena, de esto surge:

> El Carding, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacking y el Cracking, mediante los cuales se consiguen los números de las tarjetas.

2.5 OTROS HABITANTES DEL CIBERESPACIO

Según Julio Cesar Ardita, Director de Cybsec S.A. en una entrevista personal realizada en Enero de 2001 existen otras personas que pueden dañar un sistema.

2.5.1 GURÚS

Son considerados los maestros y los encargados de "formar" a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas, tales como Nicholas Negroponte (Director del “Masachusetts Institute of Technology Media Lab” o Manuel Castells (Director del “Internet Interdisciplinary Institute”)

2.5.2 LAMERS O SCRIPT-KIDDERS

Prueban todos los programas (con el título "como ser un hacker en 21 días") que llegan a sus manos. Generalmente son los responsables de soltar virus y bombas lógicas en la red sólo con el fin de molestar y que otros se enteren que usa tal o cual programa. Son aprendices que presumen de lo que no son aprovechando los conocimientos del hacker y lo ponen en práctica sin saber.

2.5.3 COPYHACKERS

Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).

2.5.4 BUCANEROS

Son comerciantes sucios que venden los productos crackeados por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los copyhackers. Son personas sin ningún (o escaso) conocimiento de informática y electrónica.

2.5.5 NEWBIE

Son los novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido.

2.5.6 WANNABER

Es aquella persona que desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consiga avanzar en sus propósitos.

2.5.7 SAMURAI

Estos saben lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers. Se basan en el principio de que cualquiera puede ser atacado y saboteado, solo basta que alguien lo desee y tenga el dinero para pagarlo.

2.5.8 PIRATAS INFORMÁTICOS

Este personaje es el realmente peligroso desde el punto de vista del Copyright, ya que copia soportes audiovisuales (discos compactos, cassettes, DVD).

2.5.9 CREADORES DE VIRUS

Si de daños y mala fama se trata estos se llevan todos los premios. Aquí, una vez más, se debe hacer la diferencia entre los creadores: que se consideran a sí mismos desarrolladores de software; y los que infectan los sistemas con los virus creados. Sin embargo es difícil imaginar que cualquier "desarrollador" no se vea complacido al ver que su "creación" ha sido ampliamente "adquirida por el público".

2.6 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70%[18] son causados por el propio personal de la organización propietaria de dichos sistemas ("Inside Factor").

La figura 2.1 detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos.

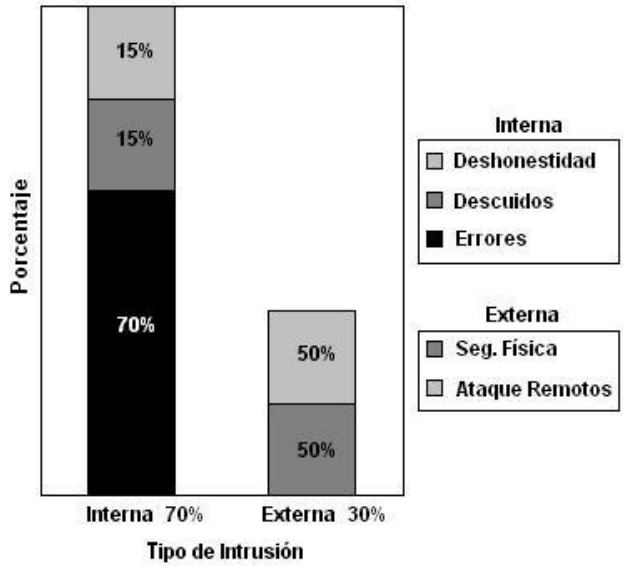

Figura 2.1 Tipo de Intrusión (2007).
http://www.cybsec.com

[18] Cybsec S.A. http://cybec.com

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar.

Existen diversos estudios que tratan sobre los motivos que llevan a una persona a cometer delitos informáticos contra su organización, pero sean cuales sean, estos motivos existen y deben prevenirse y evitarse. Suele decirse que todos tenemos un precio (dinero, chantaje, factores psicológicos), por lo que nos pueden arrastrar a robar y vender información o simplemente proporcionar acceso a terceros.

2.6.1 PERSONAL INTERNO

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema.

2.6.2 EX EMPLEADO

Este grupo puede estar especialmente interesado en violar la seguridad de la organización, sobre todo, aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia.

2.6.3 CURIOSOS

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aún no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers (podrían ser Newbies). En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él vedada. Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad con confiabilidad generado en un sistema.

2.6.4 TERRORISTAS

Bajo esta definición se engloba a cualquier persona que ataca el sistema para hacer daño de cualquier índole en él, y no solo a la persona que coloca bombas o quema automóviles. Por ejemplo el ataque de modificación[19] de los datos de clientes entre empresas competidoras, o de servidores que albergan páginas web, bases de datos entre partidos políticos contrarios.

2.6.5 INTRUSOS REMUNERADOS

Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto) o simplemente para dañar, de alguna manera la imagen de la entidad atacada.

Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

[19] Por modificación se entiende cualquier cambio de los datos incluyendo su borrado.

CAPITULO III

AMENAZAS LOGICAS

CAPITULO III AMENAZAS LOGICAS

La Entropía es una magnitud termodinámica que cuantifica el grado de desorden de un sistema; y según las leyes físicas todo sistema tiende a su máxima entropía. Si extrapolamos este concepto a la seguridad resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir:

- Los protocolos de comunicación utilizados carecen, en su mayoría, de seguridad o esta ha sido implementada, tiempo después de su creación, en forma de (parche).
- Existen agujeros de seguridad en los sistemas operativo, por ejemplo la UAC[20] de Windows 7 que advierte al usuario sobre cualquier cambio realizado en el sistema por un programa hecho por un tercero, *pero* no advierte sobre los cambios realizados en la configuración de Windows.
- Existen agujeros de seguridad en las aplicaciones; la mayor parte de las empresas no logran proteger sus sitios web y servidores contra los métodos de ataque más elementales.
- Existen errores en las configuraciones de los sistemas, la no instalación o actualización del antivirus permite que cualquier virus entre y dañe nuestro sistema.
- Los usuarios carecen de información respecto al tema, es decir, cuando no capacitamos al personal acerca de las normas de seguridad lógica existente en la organización.

3.1 ACCESO - USO - AUTORIZACIÓN

La identificación de estas palabras (acceso, uso y autorización) es muy importante ya que el uso de algunas implica un uso desapropiado de las otras. Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso.

[20] Control de Acceso de Usuario

Por ejemplo:

- Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.
- Cuando un atacante tiene acceso desautorizado está haciendo uso desautorizado del sistema.
- Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario).

Luego un ataque será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un Incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos).

3.2 IDENTIFICACIÓN DE LAS AMENAZAS

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- **Data Corruption:** La información que no contenía defectos pasa a tenerlos.
- **Denial of Service (DoS):** Servicios que deberían estar disponibles no lo están.
- **Leakage:** Los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

La tabla 3.1 detalla el tipo de atacante, las herramientas utilizadas, en qué fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

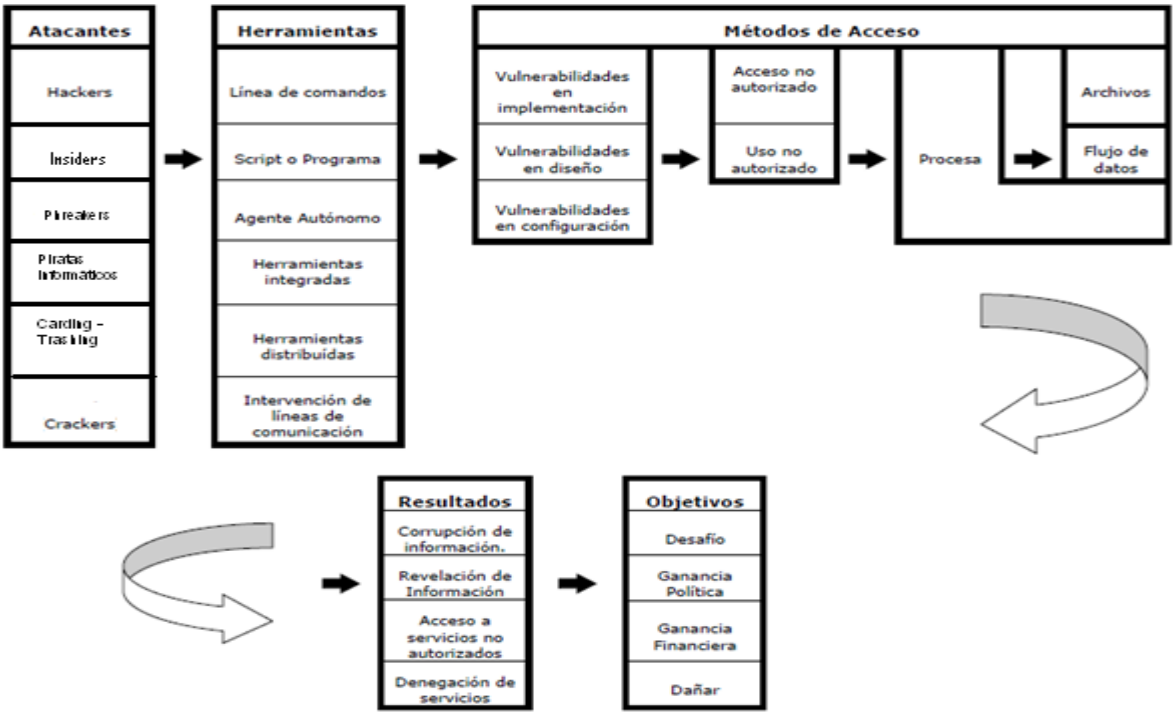

Tabla 3.1 Detalle de ataques.
HOWARD, John D. Thesis. http://www.cert.org

Cualquier adolescente de 15 años (Script Kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Los números que siguen no pretenden alarmar a nadie ni sembrar la semilla del futuro hacker (Tabla 3.2). Evidentemente la información puede ser aprovechada para fines menos lícitos que para los cuales fue pensada, pero esto es algo ciertamente difícil de evitar.

Año	**Incidentes Reportados**	**Vulnerabilidades Reportadas**	**Mensajes Recibidos**
1988	6		539
1989	132		2868
1990	252		4448

1991	4.6		9629
1992	773		14463
1993	1334		21267
1994	2340		29580
1995	2412	171	32084
1996	2573	345	31268
1997	2134	311	39626
1998	3734	262	41871
1999	9859	417	34612
2000	21756	1.090	56365
2001	52658	1417	118907
2002	82094	808	204841
2003	137529	934	542754
2004	--------	795	717863
2005	---------	591	624634
2006	----------	977	674235
Total	**319992**	**24464**	**3201855**

Tabla 3.2 Vulnerabilidades reportadas al CERT 1988-2006.
CERT Internacional. http://www.cert.org/stats/

3.3 TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar debilidades en el diseño, configuración y operación de los sistemas.

3.3.1 INGENIERA SOCIAL (IS)

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente (generalmente es así), puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

Para evitar situaciones de IS es conveniente tener en cuenta estas recomendaciones:

- Tener servicio técnico propio o de confianza.
- Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y deriven la inquietud a los responsables que tenga competencia para dar esa información.
- Asegurarse que las personas que llaman por teléfono son quien dicen ser. Por ejemplo si la persona que llama se identifica como proveedor de Internet lo mejor es cortar y devolver la llamada a forma de confirmación.

3.3.2 INGENIERÍA SOCIAL INVERSA (ISI)

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema). La ISI es más difícil de llevar a cabo y por lo general se aplica cuando los usuarios están alertados de acerca de las técnicas de IS. Puede usarse en algunas situaciones específicas y después de mucha preparación e investigación por parte del intruso:

1. Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruso tenga un mínimo contacto con el sistema.
2. Comunicación a los usuarios de que la solución es brindada por el intruso (publicidad).
3. Provisión de ayuda por parte del intruso encubierto como servicio técnico.

3.3.3 TRASHING

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema.

El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc. El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

3.3.4 ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

3.3.5 ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

3.3.6 DENIAL OF SERVICE (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un "crash" del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede "matar" en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DoS deteniendo los servicios.

3.3.7 ATAQUES DE MODIFICACIÓN-DAÑO

3.3.7.1 TAMPERING O DATA DIDDLING

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos. Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

Aún así, si no hubo intenciones de bajar el sistema por parte del atacante; el administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por Insiders o Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva.

Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA o la modificación del Web Site del CERT (mayo de 2001). Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.). La utilización de programas troyanos y difusión de virus esta dentro de esta categoría.

3.3.7.2 BORRADO DE HUELLAS

El borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo.

Los archivos logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

3.3.7.3 VULNERABILIDADES EN LOS NAVEGADORES

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los "Buffer Overflow[21]".

Los "Buffer Overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

Los protocolo usado puede ser HTTP, pero también otros menos conocidos, internos de cada explorador, como el *"res:"* o el *"mk:"*. Precisamente existen fallos de seguridad del tipo "Buffer Overflow" en la implementación de estos dos protocolos.

[21] http://www.newhackcity.net/win_buff_overflow

Además de las vulnerabilidades del tipo Transversal en el servidor Web Internet Information Server de la empresa Microsoft (octubre 2000) , explotando fallas en la traducción de caracteres Unicode, puso de manifiesto cuan fácil puede resultar explotar una cadena no validada. Por ejemplo:
www.servidor.com/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

Devuelve el directorio de la unidad c: del servidor deseado.

Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje Assembler y de la estructura interna de la memoria del sistema operativo utilizado o bien, leer la documentación de sitios web donde explican estas fallas.

También se puede citar el fallo de seguridad descubierto por Cybersnot Industries relativo a los archivos "*.lnk"* y "*.url"*de Windows 95 y NT respectivamente. Algunas versiones de Microsoft Internet Explorer podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima (por ejemplo el tan conocido y temido *format.com*).

3.3.8 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informáticos disponibles.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows). La importancia y ventaja del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente se encuentran en Internet avisos de nuevos descubrimientos de problemas de seguridad, herramientas de Hacking y Exploits que los explotan, por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

3.3.9 IMPLEMENTACIÓN DE ESTAS TÉCNICAS

A lo largo de la investigación se ha recopilando distinto tipos de programas que son la aplicación de las distintas técnicas enumeradas anteriormente. La mayoría de los mismos son encontrados fácilmente en Internet en versiones ejecutables, y de otros se encuentra el código fuente, generalmente en lenguaje C, Java y Perl. Cada una de las técnicas explicadas puede ser utilizadas por un intruso en un ataque.

A continuación se establece el orden de utilización de las mismas, pero siempre remarcando que un ataque insume mucha paciencia, imaginación acumulación de conocimientos y experiencia dada, en la mayoría de los casos por prueba y error.

1. Identificación del problema (víctima): en esta etapa se recopila toda la información posible de la víctima. Cuanta más información se acumule, más exacto y preciso será el ataque, más fácil será eliminar las evidencias y más difícil será su rastreo.
2. Exploración del sistema víctima elegido: en esta etapa se recopila información sobre los sistemas activos de la víctima, cuales son los más vulnerables y cuales se encuentran disponibles. Es importante remarcar que si la victima parece apropiada en la etapa de Identificación, no significa que esto resulte así en esta segunda etapa.
3. Enumeración: en esta etapa se identificaran las cuentas activas y los recursos compartidos mal protegidos. La diferencia con las etapas anteriores es que aquí se establece una conexión activa a los sistemas y la realización de consultas dirigidas.

Estas intrusiones pueden (y deberían) ser registradas, por el administrador del sistema, o al menos detectadas para luego ser bloqueadas.

4. Intrusión propiamente dicha: en esta etapa el intruso conoce perfectamente el sistema y sus debilidades y comienza a realizar las tareas que lo llevaron a trabajar, en muchas ocasiones, durante meses.

Contrariamente a lo que se piensa, los sistemas son difíciles de penetrar si están bien administrados y configurados. Ocasionalmente los defectos propios de la arquitectura de los sistemas proporciona un fácil acceso, pero esto puede ser, en la mayoría de los casos, subsanado aplicando las soluciones halladas.

3.3.10 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.

4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como multiplicadores durante un ataque Smurf.
5. Auditorias de seguridad y sistemas de detección.
6. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados
7. Por último, la capacitación continúa del usuario.

3.4 CREACIÓN Y DIFUSIÓN DE VIRUS

Quizás uno de los temas más famosos y sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los Virus.

Pero como siempre en esta obscura realidad existe una parte que es cierta y otra que no lo es tanto. Para aclarar este enigma veamos porque se eligió la palabra virus (del latín Veneno) y que son realmente estos "parásitos".

3.4.1 VIRUS INFORMÁTICOS

Virus Informático (VI): Pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica). "Un virus responde al modelo DAS: Dañino, Autorreplicante y Subrepticio."[22]

3.4.2 MODELO DE VIRUS INFORMÁTICO

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

[22] Dr. Fred Cohen. Considerado el padre de los VI y de sus técnicas de defensa: http://all.net

1. **Módulo de Reproducción:** es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticiamente, permitiendo su transferencia a otras computadoras.
2. **Módulo de Ataque:** Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.
3. **Módulo de Defensa:** Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus (Figura 3.1).

Figura 3.1 - Módulos de los Virus Informáticos
CERT Internacional. http://www.cert.org/stats/

3.4.3 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS

Los virus informáticos no afectan (en su gran mayoría) directamente el hardware sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la siguiente clasificación se ha tenido en cuenta que el daño es una acción de la computadora, no deseada por el usuario:

a. **Daño Implícito:** Es el conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar su accionar y propagación. Aquí se debe considerar el entorno en el que se desenvuelve el virus ya que el consumo de ciclos de reloj en un medio delicado (como un aparato biomédico) puede causar un gran daño.
b. **Daño Explícito:** Es el que produce la rutina de daño del virus.

Con respecto al modo y cantidad de daño, encontramos:

a. **Daños triviales:** Daños que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario. Deshacerse del virus implica, generalmente, muy poco tiempo.
b. **Daños menores:** Daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos. En el peor de los casos se tendrá que reinstalar las aplicaciones afectadas.
c. **Daños moderados:** Los daños que el virus provoca son formatear el disco rígido o sobrescribir parte del mismo. Para solucionar esto se deberá utilizar la última copia de seguridad que se ha hecho y reinstalar el sistema operativo.
d. **Daños mayores:** Algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad también infectadas. Puede que se llegue a encontrar una copia de seguridad no infectada, pero será tan antigua que se haya perdido una gran cantidad de archivos que fueron creados con posterioridad.
e. **Daños severos**: Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No se sabe cuando los datos son correctos o han cambiado, pues no hay unos indicios claros de cuando se ha infectado el sistema.
f. **Daños ilimitados:** El virus "abre puertas" del sistema a personas no autorizadas. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en el sistema.

3.4.4 TÉCNICAS DE PROPAGACIÓN

Actualmente las técnicas utilizadas por los virus para logra su propagación y subsistencia son muy variadas y existen aquellos que utilizan varias de ellas para lograrlo.

1. Disquetes y otros medios removibles. A la posibilidad de que un disquete contenga un archivo infectado se une el peligro de que integre un virus de sector de arranque (Boot). En este segundo caso, y si el usuario lo deja en la disquetera, infectará el ordenador cuando lo encienda, ya que el sistema intentará arrancar desde el disquete.
2. Correo electrónico: el usuario no necesita hacer nada para recibir mensajes que, en muchos casos ni siquiera ha solicitado y que pueden llegar de cualquier lugar del mundo. Los mensajes de correo electrónico pueden incluir archivos, documentos o cualquier objeto infectado que, al ejecutarse, contagian la computadora del usuario. En las últimas generaciones de virus se envían e-mails sin mensajes pero con archivos adjuntos (virus) que al abrirlos proceden a su ejecución y posterior infección del sistema atacado. Estos virus poseen una gran velocidad de propagación ya que se envían automáticamente a los contactos de la libreta de direcciones del sistema infectado.
3. IRC o Chat: las aplicaciones de mensajería instantánea (ICQ, AOL Instant Messenger, etc.) o Internet Relay Chat (IRC), proporcionan un medio de comunicación anónimo, rápido, eficiente, cómodo y barato. Sin embargo, también son peligrosas, ya que los entornos de chat ofrecen, por regla general, facilidades para la transmisión de archivos, que conllevan un gran riesgo en un entorno de red.
4. Páginas web y transferencia de archivos vía FTP: los archivos que se descargan de Internet pueden estar infectados, y pueden provocar acciones dañinas en el sistema en el que se ejecutan.
5. Grupos de noticias: sus mensajes e información (archivos) pueden estar infectados y, por lo tanto, contagiar al equipo del usuario que participe en ellos.

3.4.5 TIPOS DE VIRUS

Un virus puede causar daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada y nadie en su sano juicio deseará ejecutarlo. Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para que su "programa" pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas:

3.4.5.1 ARCHIVOS EJECUTABLE (VIRUS EXEVIR)

El virus se adosa a un archivo ejecutable y desvía el flujo de ejecución a su código, para luego retornar al huésped y ejecutar las acciones esperadas por el usuario. Al realizarse esta acción el usuario no se percata de lo sucedido. Una vez que el virus es ejecutado se aloja en memoria y puede infectar otros archivos ejecutables que sean abiertos en esa máquina (Figura 3.2).

En este momento su dispersión se realiza en sistema de 16 bits (DOS) y de 32 bits (Windows) indistintamente, atacando programas .COM, .EXE, .DLL, .SYS, .PIF, etc, según el sistema infectado.

Ejemplos:

- Chernobyl (Borra el contenido del disco duro e impide el arranque de la computadora, así como infecta ficheros con extensión EXE y en ocasiones borra el contenido de la BIOS)
- Darth Vader (Este virus sobre escribe parte del fichero que infecta y se reproduce insertando su código en otros archivos o programas)
- PHX (este busca una computadora en particular y si la encuentra, borra información específica de esa máquina)

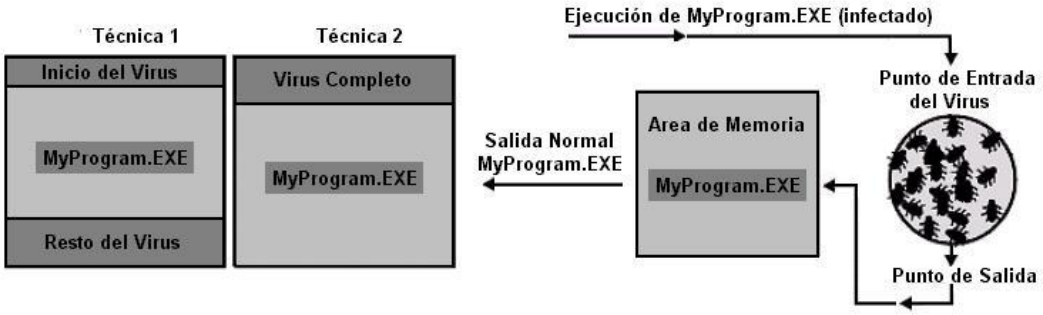

Figura 3.2 - Técnicas de Infección en Archivos Ejecutables
CERT Internacional. http://www.cert.org/stats/

3.4.5.2 VIRUS EN EL SECTOR DE ARRANQUE (VIRUS ACSO ANTERIOR A LA CARGA DEL SO)

En los primeros 512 bytes de un disquete formateado se encuentran las rutinas necesarias para la carga y reconocimiento de dicho disquete. Entre ellas se encuentra la función invocada si no se encuentra el Sistema Operativo. Es decir que estos 512 bytes se ejecutan cada vez que se intenta arrancar (bootear) desde un disquete (o si se dejó olvidado uno en la unidad y el orden de booteo de la PC es A: y luego C:). Luego, esta área es el objetivo de un virus de booteo (Figura 3.3)

Se guarda la zona de booteo original en otro sector del disco (generalmente uno muy cercano o los más altos). Luego el virus carga la antigua zona de booteo. Al arrancar el disquete se ejecuta el virus (que obligatoriamente debe tener 512 bytes o menos) quedando residente en memoria; luego ejecuta la zona de booteo original, salvada anteriormente. Una vez más el usuario no se percata de lo sucedido ya que la zona de booteo se ejecuta iniciando el sistema operativo (si existiera) o informando la falta del mismo.

Ejemplos:

- Stoned: Infecta los sistemas de arranque tanto de los disquetes como de los discos duros, este solo puede contagiar al master boot del disco duro arrancando o iniciando desde un disquete infectado.

- Diablo: Infecta los sistemas de arraque de la master boot, es de baja peligrosidad y afecta computadoras con sistema operativo Windows, en una de sus variantes afecta a paquetería de oficina (Excel) creando una archivo desde el cual se ejecuta el virus.
- Michelangelo : Infecta los sectores de arranque de los disquetes y de los discos duros, el principal síntoma visible de que se está ejecutando este virus aparecen el día 6 de marzo o después de esta fecha.
- 512: Infecta el sector de arranque de los discos duros y el de los disquetes. Este virus es residente, está parcialmente encriptado y utiliza técnicas de ocultamiento. El 2 de mayo, el virus bloquea el teclado del ordenador infectado y muestra un mensaje en pantalla.

Figura 3.3 - Técnica de infección en Zona de Booteo
CERT Internacional. http://www.cert.org/stats/

3.4.5.3 VIRUS RESIDENTE

Un virus puede residir en memoria. El objetivo de esta acción es controlar los accesos a disco realizados por el usuario y el Sistema Operativo. Cada vez que se produce un acceso, el virus verifica si el disco o archivo objetivo al que se accede, está infectado y si no lo está procede a almacenar su propio código en el mismo. Este código se almacenará en un archivo, tabla de partición, o en el sector de booteo, dependiendo del tipo de virus que se trate.

Ejemplos:

- Michelangelo (Fue diseñado para infectar el BIOS y dañado los sectores de arranque)
- DIR II. (infecta archivos con terminación COM y EXE y cambia las entradas de directorios)

3.4.5.4 MACROVIRUS

Estos virus infectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Últimamente son los más expandidos, ya que todos los usuarios necesitan hacer intercambio de documentos para realizar su trabajo. Las suficientemente poderosas como permitir este tipo de implementación. Pero los primeros de difusión masiva fueron desarrollados a principios de los ´90 para el procesador de texto Microsoft Word , ya que este cuenta con el lenguaje de programación Word Basic (Figura 1.8).

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macrovirus.

Ejemplos:

De Microsoft Word: CAP I, CAP II, Concept, Wazzu.

De Microsoft Excel: Laroux.

De Lotus Amipro: GreenStripe

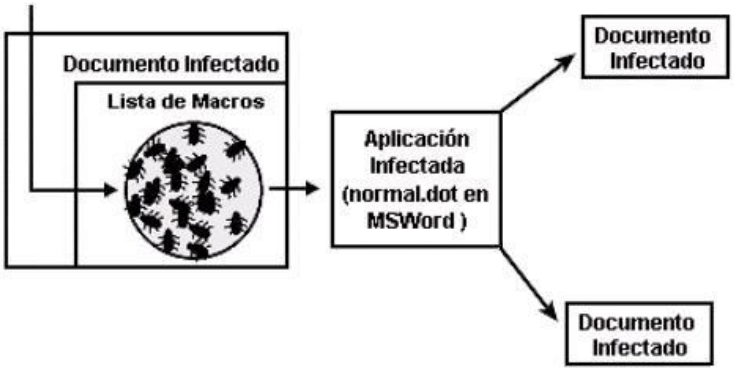

Figura 3.4 - Infección de múltiples Documentos
CERT Internacional. http://www.cert.org/stats/

3.4.5.5 VIRUS DE MAIL

La manera de actuar, al igual que los anteriores, se basa en la confianza excesiva por parte del usuario: a este le llega vía mail un mensaje con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

Este tipo de virus tomó relevancia estos últimos años con al explosión masiva de Internet y últimamente con el virus Melissa y I Love You. Generalmente estos virus se auto envían a algunas de las direcciones de la libreta. Cada vez que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.

3.4.5.6 VIRUS DE SABOTAJE

Son virus construidos para sabotear un sistema o entorno específico. Requieren de conocimientos de programación pero también una acción de inteligencia que provea información sobre el objetivo y sus sistemas.

3.4.5.7 HOAX, LOS VIRUS FANTASMAS

El auge del correo electrónico generó la posibilidad de transmitir mensajes de alerta de seguridad.

Así comenzaron a circular mensajes de distinta índole (virus, cadenas solidarias, beneficios, catástrofes, etc.) de casos inexistentes. Los objetivos de estas alertas pueden causar alarma, la pérdida de tiempo, el robo de direcciones de correo y la saturación de los servidores con las consecuentes pérdidas de dinero que esto ocasiona.

3.4.5.8 VIRUS DE APPLETS JAVA Y CONTROLES ACTIVEX

Si bien, como ya se comentó, estas dos tecnologías han sido desarrolladas teniendo como meta principal la seguridad, la práctica demuestra que es posible programar virus sobre ellas. Este tipo de virus se copian y se ejecutan a sí mismos mientras el usuario mantiene una conexión a Internet.

3.4.5.9 REPRODUCTORES-GUSANOS

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

3.4.5.10 CABALLOS DE TROYA

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocía, y que tenía una función muy diferente a la que ellos podían imaginar; un Caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

Si bien este tipo de programas no cumplen con la condición de auto-reproducción de los virus, encuadran perfectamente en la características de programa dañino. Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

Los ejemplos más conocidos de troyanos son el Back Oriffice y el Net Bus que, si bien no fueron desarrollados con ese fin, son una poderosa arma para tomar el control de la computadora infectada. Estos programas pueden ser utilizados para la administración total del sistema atacado por parte de un tercero, con los mismos permisos y restricciones que el usuario de la misma.

3.4.5.11 BOMBAS LÓGICAS

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada o dado algún evento particular en el sistema, bien destruye y modifica la información o provoca la baja del sistema.

3.4.6 PROGRAMA ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Actualmente existen técnicas, conocidas como heurísticas, que brindan una forma de "adelantarse" a los nuevos virus. Con esta técnica el antivirus es capaz de analizar archivos y documentos y detectar actividades sospechosas. Esta posibilidad puede ser explotada gracias a que de los 6-20 nuevos virus diarios, sólo aparecen unos cinco totalmente novedosos al año.

Debe tenerse en cuenta que:

- Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.
- No será eficaz el 100% de los casos, no existe la protección total y definitiva.

Las funciones presentes en un antivirus son:

1. **Detección:** se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
2. **Identificación de un virus:** existen diversas técnicas para realizar esta acción:

a. **Scanning**: técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos del antivirus. Su principal ventaja reside en la rápida y exacta que resulta la identificación del virus.

   En los primeros tiempos (cuando los virus no eran tantos ni su dispersión era tan rápida), esta técnica fue eficaz, luego se comenzaron a notar sus deficiencias. El primer punto desfavorable es que brinda una solución a posteriori y es necesario que el virus alcance un grado de dispersión considerable para que llegue a mano de los investigadores y estos lo incorporen a su base de datos (este proceso puede demorar desde uno a tres meses). Este modelo reactivo jamás constituirá una solución definitiva.

b. Heurística*:* búsqueda de acciones potencialmente dañinas perteneciente a un virus informático. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controlada por el usuario (MBR, Boot Sector, FAT, y otras). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a las base de datos de los antivirus (técnica proactiva). Su desventaja radica en que puede "sospechar" de demasiadas cosas y el usuario debe ser medianamente capaz de identificar falsas alarmas.

3. **Chequeadores de Integridad**: Consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma.

   Su ventaja reside en la prevención aunque muchas veces pueden ser vulnerados por los virus y ser desactivados por ellos, haciendo que el usuario se crea protegido, no siendo así.

Es importante diferencia los términos detectar: determinación de la presencia de un virus e identificar: determinación de qué virus fue el detectado.

Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

3.4.6.1 MODELO DE UN ANTIVIRUS

Un antivirus puede estar constituido por dos módulos principales y cada uno de ellos contener otros módulos (Figura 3.5).

Figura 3.5 Modelo de un antivirus
CERT Internacional. http://www.cert.org/stats/

- **Módulo de Control:** Este módulo posee la técnica de Verificación de Integridad que posibilita el registro de posibles cambios en los zonas y archivos considerados de riesgo.
- **Módulo de Respuesta:** La función de "Alarma" se encuentra en todos los antivirus y consiste en detener la ejecución de todos lo programas e informar al usuario de la posible existencia de un virus. La mayoría ofrecen la posibilidad de su erradicación si la identificación a sido positiva.

CAPITULO IV

HERRAMIENTAS DE PROTECCION

CAPITULO IV HERRAMIENTOS DE PROTECCION

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades estudiadas son el resultado de implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

En el presente capítulo, después de lo expuesto y vistas la gran cantidad de herramientas con las que cuenta el intruso, es el turno de estudiar implementaciones en la búsqueda de mantener el sistema seguro.

Siendo reiterativos, ninguna de las técnicas expuestas a continuación representarán el 100% de la seguridad deseado, aunque muchas parezcan la panacea, será la suma de algunas de ellas las que convertirán un sistema interconectado en confiable.

4.1 VULNERAR PARA PROTEGER

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder colarse en ella. El trabajo de los administradores y testers no difiere mucho de esto. En lo que sí se diferencia, y por completo, es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo) un administrador lo hace para poder mejorar los sistemas de seguridad.

Los intrusos cuentan con grandes herramientas como los scanners, los cracking de passwords, software de análisis de vulnerabilidades y los exploits; un administrador de sistema cuenta con todas ellas empleadas para bien, los logs, los sistemas de detección de intrusos y los sistemas de rastreo de intrusiones[23]".

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como penetration testing[24], uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Un test está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; no a la inversa. El software y el Hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina políticas de seguridad internas que cada organización (y usuario) debe generar e implementar.

4.1.1 ADMINISTRACIÓN DE LA SEGURIDAD

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

- **Autenticación:** Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- **Autorización:** es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **Auditoría:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

[23] http://ww.cybsec.com
[24] ARDITA, Julio Cesar. Director de Cybsec S.A. Security System y Ex-hacker

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda (proactividad). A continuación se citan algunos de los métodos de protección más comúnmente empleados:

1. **Sistemas de detección de intrusos:** Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. **Sistemas orientados a conexión de red:** Monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.
3. **Sistemas de análisis de vulnerabilidades:** Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
4. **Sistemas de protección a la integridad de información:** Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.

5. **Sistemas de protección a la privacidad de la información:** Herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Podemos considerar que estas capas son:

1. Política de seguridad de la organización.
2. Auditoría.
3. Sistemas de seguridad a nivel de Router-Firewall.
4. Sistemas de detección de intrusos.
5. Plan de respuesta a incidentes.
6. Penetration Test.

4.1.2 PENETRATION TEST, ETHICAL HACKING O PRUEBA DE VULNERABILIDAD

El Penetration Test es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos."[25]

El objetivo del Penetration Test es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos.

[25] ARDITA, Julio Cesar. "Prueba de Vulnerabilidad". 1996-2001 CYBSEC S.A. http://www.cybsec.com/0302.htm

También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El Penetration Test se compone de dos grandes fases de testeo:

Penetration Test Externo: el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:

- Pruebas de usuarios y la "fuerza" de sus passwords.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Scanning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Prueba de ataques de Denegación de Servicio.

Penetration Test Interno: este tipo de testeo trata de demostrar cual es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.

- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio

3.1.3 HONEYPOTS-HONEYNETS

Estas trampas de red son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su hábitat natural. Actualmente un equipo de Honeynet Project[26] trabaja en el desarrollo de un documento sobre la investigación y resultados de su trampa, la cual fue penetrada a la semana de ser activada (sin publicidad).

Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos. Ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los fascinantes programas que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen", dijo Dan Adams.[27]

4.2 FIREWALLS

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad (Figura 4.1).

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders.

[26] Honeynet Project: http://project.honeynet.org
[27] ADAMS, Dan. Administrador de los sistemas London SecTech, quien sigue de cerca el proyecto Honeynet.

Un firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

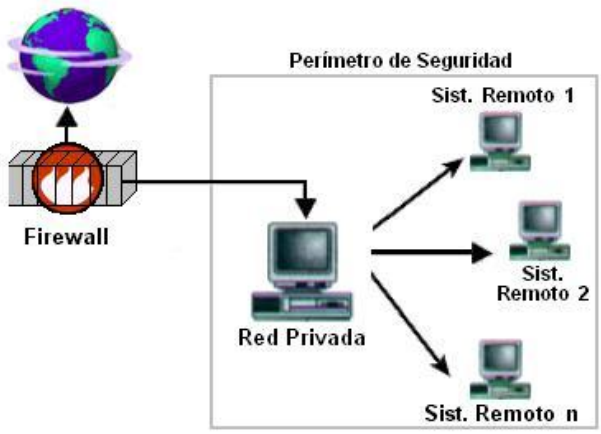

Figura 4.1 – Firewall
Honeynet Project: http//Project.honeynet.org

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red.

Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación.

4.2.1 POLÍTICAS DE DISEÑO DE FIREWALLS

Las políticas de accesos en un firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.

Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

- ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

a. Paradigmas de seguridad

- Se permite cualquier servicio excepto aquellos expresamente prohibidos.
- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.

b. Estrategias de seguridad

- Paranoica: se controla todo, no se permite nada.

- Prudente: se controla y se conoce todo lo que sucede.
- Permisiva: se controla pero se permite demasiado.
- Promiscua: no se controla (o se hace poco) y se permite todo.
- ¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuánto es conveniente invertir.

4.2.2 BENEFICIOS DE UN FIREWALL

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todos las computadoras de la red estarían expuestos a ataques desde el exterior.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible. Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

4.3 ACCESS CONTROL LISTS (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos.

Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

4.4 WRAPPERS

Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica está concentrada en un solo programa, los Wrappers son fáciles y simples de validar.
- Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el Wrapper.
- Debido a que los Wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de Logs y auditorias de peticiones a dichos servicios, ya sean autorizados o no.

El paquete Wrapper más ampliamente utilizado es el TCP-Wrappers, el cual es un conjunto de utilidades de distribución libre, escrito por Wietse Venema (co-autor de SATAN, con Dan Farmer, y considerado el padre de los sistemas Firewalls) en 1990.

Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio. Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Algunas configuraciones avanzadas de este paquete, permiten también ejecutar comandos en el propio sistema operativo, en función de la resolución de la petición. Por ejemplo, es posible que interese detectar una posible máquina atacante, en el caso de un intento de conexión, para tener más datos a la hora de una posible investigación.

4.5 DETECCIÓN DE INTRUSOS EN TIEMPO REAL

La seguridad se tiene que tratar en conjunto. Este viejo criterio es el que recuerda que los sistemas de protección hasta aquí abordados, si bien son eficaces, distan mucho de ser la protección ideal.

Así, debe estar fuera de toda discusión la conveniencia de añadir elementos que controlen lo que ocurre dentro de la red (detrás de los Firewalls).

Como se ha visto, la integridad de un sistema se puede corromper de varias formas y la forma de evitar esto es con la instalación de sistemas de Detección de Intrusos en Tiempo Real, quienes:

- Inspeccionan el tráfico de la red buscando posibles ataques.
- Controlan el registro de los servidores para detectar acciones sospechosas (tanto de intrusos como de usuarios autorizados).
- Mantienen una base de datos con el estado exacto de cada uno de los archivos (Integrity Check) del sistema para detectar la modificación de los mismos.
- Controlan el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.

- Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones del mismo.
- Avisan al administrador de cualquiera de las acciones mencionadas.

Cada una de estas herramientas permiten mantener alejados a la gran mayoría de los intrusos normales.

Algunos con suficientes conocimientos, experiencia y paciencia serán capaces de utilizar métodos sofisticados (u originales) como para voltear el perímetro de seguridad (interna + externa) y serán estos los casos que deban estudiarse para integrar a la política de seguridad existente mayor conocimiento y con él mayor seguridad.

4.5.1 INTRUSIÓN DETECTION SYSTEMS (IDS)

Un sistema de detección de intrusos es un componente más dentro del modelo de seguridad de una organización. Consiste en detectar actividades inapropiadas, incorrectas desde el exterior-interior de un sistema informático.

Los sistemas de detección de intrusos pueden clasificarse, según su función y comportamiento en:

- **Host-Based IDS**: Operan en un host para detectar actividad maliciosa en el mismo.
- **Network-Based IDS**: Operan sobre los flujos de información intercambiados en una red.
- **Knowledge-Based IDS**: Sistemas basados en Conocimiento.
- **Behavior-Based IDS**: Sistemas basados en Comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuará como un usuario comprometido; su comportamiento se alejará del de un usuario normal.

Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Así las intrusiones pueden clasificarse en:

- **Intrusivas pero no anómalas:** Denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema.
- **No intrusivas pero anómalas:** Denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados.
- **No intrusiva ni anómala:** son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
- **Intrusiva y anómala:** se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada.

Los detectores de intrusiones anómalas requieren mucho gasto computacional, ya que se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

4.5.1.1 CARACTERÍSTICAS DE IDS

Cualquier sistema de detección de intrusos debería, sea cual sea el mecanismo en que esté basado, debería contar con las siguientes características:

- Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado. Sin embargo, no debe ser una "caja negra" (debe ser examinable desde el exterior).
- Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.
- En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
- Debe imponer mínima sobrecarga sobre el sistema. Un sistema que minimiza el rendimiento de la máquina, simplemente no será utilizado.
- Debe observar desviaciones sobre el comportamiento estándar.
- Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
- Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.
- Debe ser difícil de "engañar".

4.5.1.2 FORTALEZAS DE IDS

- Suministra información muy interesante sobre el tráfico malicioso de la red.
- Poder de reacción para prevenir el daño.
- Es una herramienta útil como arma de seguridad de la red.
- Ayuda a identificar de dónde provienen los ataques que se sufren.
- Recoge evidencias que pueden ser usadas para identificar intrusos.
- Es una "cámara" de seguridad y una "alarma" contra ladrones.
- Funciona como "disuasor de intrusos".
- Alerta al personal de seguridad de que alguien está tratando de entrar.
- Protege contra la invasión de la red.
- Suministra cierta tranquilidad.
- Es una parte de la infraestructura para la estrategia global de defensa.

- La posibilidad de detectar intrusiones desconocidas e imprevistas.
- Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques.
- Son menos dependientes de los mecanismos específicos de cada sistema operativo.
- Pueden ayudar a detectar ataques del tipo "abuso de privilegios" que no implica realmente ninguna vulnerabilidad de seguridad. En pocas palabras, se trata de una aproximación a la paranoia: "todo aquello que no se ha visto previamente es peligroso".
- Menor costo de implementación y mantenimiento al ubicarse en puntos estratégicos de la red.
- Dificulta el trabajo del intruso de eliminar sus huellas.

4.5.1.3 DEBILIDADES DE IDS

- No existe un parche para la mayoría de bugs de seguridad.
- Se producen falsas alarmas.
- Se producen fallos en las alarmas.
- No es sustituto para un buen Firewall, una auditoría de seguridad regular y una fuerte y estricta política de seguridad.

4.5.1.4 INCONVENIENTES DE IDS

- La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje.
- El comportamiento puede cambiar con el tiempo, haciendo necesario un re-entrenamiento periódico del perfil, lo que da lugar a la no disponibilidad del sistema o la generación de falsas alarmas adicionales.
- El sistema puede sufrir ataques durante la fase de aprendizaje, con lo que el perfil de comportamiento contendrá un comportamiento intrusivo el cual no será considerado anómalo.

4.6 CALL BACK

Este procedimiento es utilizado para verificar la autenticidad de una llamada vía modem. El usuario llama, se autentifica contra el sistema, se desconecta y luego el servidor se conecta al número que en teoría pertenece al usuario.

La ventaja reside en que si un intruso desea hacerse pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada-retorno proceda del número a donde llamó previamente.

4.7 SISTEMAS ANTI-SNIFFERS

Esta técnica consiste en detectar sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando (recordar que un sniffer la coloca en Modo Promiscuo), y el tráfico de datos en ella.

4.8 GESTION DE CLAVES "SEGURAS"

Si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo).

Esto se obtiene a partir de las 96 (7.213.895.789.838.340) claves posibles de generar con esos caracteres.

Según demuestra el análisis de +NetBuL[28] realizado sobre 2.134 cuentas y probando 227.000 palabras por segundo:

- Con un diccionario 2.030 palabras (el original de John de Ripper 1.04), se obtuvieron 36 cuentas en solo 19 segundos (1,77%).
- Con un diccionario de 250.000 palabras, se obtuvieron 64 cuentas en 36:18 minutos (3,15%).

[28] +NetBul. Tabla de tiempos del John the Ripper 1.4. http://www.vanhackez.co/set - http://www.thepentagon.com/paseante

4.8.1 NORMAS DE ELECCIÓN DE CLAVES

Se debe tener en cuenta los siguientes consejos:

1. No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
2. No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).
3. Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
4. Deben ser largas, de 8 caracteres o más.
5. Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
6. Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:

- Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3
- Usar un acrónimo de alguna frase fácil de recordar: A rio Revuelto Ganancia de Pescadores - ArRGdP
- Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P
- Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña - aHoeIlo
- Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar
- Realizar reemplazos de letras por signos o números: En Seguridad Más Vale Prevenir que Curar - 35M\/Pq< .

4.8.2 NORMAS PARA PROTEGER UNA CLAVE

La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

La siguiente frase difundida en UseNet resume algunas de las reglas básicas de uso de la contraseña: "Un password debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y NO lo compartas con tus amigos".

Algunos consejos a seguir:

- No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente.
- No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Root, System, Test, Demo, Guest, etc.
- Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
- No teclear la contraseña si hay alguien mirando.
- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "mi clave es:".

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

1. Número de intentos limitado. Tras un número de intentos fallidos, pueden tomarse distintas medidas:
   - Obligar a reescribir el nombre de usuario (lo más común).
   - Bloquear el acceso durante un tiempo.
   - Enviar un mensaje al administrador y/o mantener un registro especial.
2. Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).
3. Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.
4. Envejecimiento y expiración de contraseñas. Cada cierto tiempo se fuerza a cambiar la contraseña.

Se obliga a no repetir ciertas cantidad de las anterior. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.

5. Ataque preventivo. Muchos administradores utilizan crackeadores para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

4.8.3 CONTRASEÑAS DE UN SÓLO USO

Las contraseñas de un solo uso (One-Time Passwords) son uno de los mecanismos de autentificación más seguros, debido a que su descubrimiento tan solo permite acceder al sistema una vez. Además, en muchas ocasiones se suelen utilizar dispositivos hardware para su generación, lo que las hace mucho más difíciles de descubrir.

Ejemplos de este tipo de contraseñas serian las basadas en funciones unidireccionales (sencillas de evaluar en un sentido pero imposible o muy costoso de evaluar en sentido contrario) y en listas de contraseñas.

Se distinguen tres tipos de contraseñas de un solo uso:

1. Las que requieren algún dispositivo hardware para su generación, tales como calculadoras especiales o tarjetas inteligentes (Token Cards).
2. Las que requieren algún tipo de software de cifrado especial.
3. Las que se basan en una lista de contraseñas sobre papel.

La tarjeta genera periódicamente valores mediante a una función secreta unidireccional, basada en el tiempo y en el número de identificación de la misma. El usuario combina en número generado por la tarjeta con su palabra de paso para obtener el password de entrada, de lo que le protege en caso de robo o perdida.

4.9 SEGURIDAD EN PROTOCOLOS Y SERVICIOS

Son aquellas reglas que gobiernan las comunicaciones diseñadas para que el sistema pueda soportar ataques de carácter malicioso[29].

Como puede preverse todos estos protocolos tienen su debilidad ya sea en su implementación o en su uso. A continuación se describen los protocolos más comunes:

4.9.1 NETBIOS

Estos puertos (137-139 en TCP y UDP) son empleados en las redes Microsoft para la autentificación de usuarios y la compartición de recursos. Como primera medida debe minimizarse la cantidad de recursos compartidos y luego debe evitarse permitir el acceso global a esos dispositivos, ya que es posible el acceso de intrusos desde cualquier lugar externo a la red.

4.9.2 ICMP

A fin de prevenir los ataques basados en bombas ICMP, se deben filtrar todos los paquetes de redirección y los paquetes inalcanzables.

4.9.3 FINGER

Finger (puerto 79 en TCP), este protocolo proporciona información detallada de los usuarios de una estación de trabajo, estén o no conectados en el momento de acceder al servicio como: datos del usuario, hábitos de conexión, cuentas inactivas.

4.9.4 POP

El servicio POP[30] (puertos 109 y 110 en TCP) utilizado para que los usuarios puedan acceder a su correo sin necesidad de montar un sistemas de archivos compartidos. Mediante POP se genera un tránsito peligroso de contraseñas a través de la red.

[29] http://redalyc.uaemex.mx
[30] Post Office Protocol (POP3, *Protocolo de la oficina de correo*)

Se ofrece tres modelos distintos de autenticación: uno basado en Kerberos, apenas utilizado, otro basado en un protocolo desafío-respuesta, y el otro basado en un simple nombre de usuario con su password correspondiente.

4.9.5 NNTP

El servicio NNTP[31] (puerto 119 en TCP) es utilizado para intercambiar mensajes de grupos de noticias entre servidores de News. Los diferentes demonios encargados de esta tarea suelen discriminar conexiones en función de la dirección o el nombre de la máquina cliente para decidir si ofrece el servicio a un determinado host, y si es así, concretar de qué forma puede acceder a él (sólo lectura, sólo ciertos grupos).

De esta forma, los servidores NNTP son muy vulnerables a cualquier ataque que permita falsear la identidad de la máquina origen, como el IP Spoofing.

4.9.6 NTP

NTP (puerto 123 en UDP y TCP) es un protocolo utilizado para sincronizar relojes de máquinas de una forma muy precisa; a pesar de su sofisticación no fue diseñado con una idea de robustez ante ataques, por lo que puede convertirse en una gran fuente de problemas si no está correctamente configurado.

Son muchos los problemas de seguridad relacionados con un tiempo correcto; el más simple y obvio es la poca fiabilidad que ofrecerá el sistema de Log a la hora de determinar cuándo sucedió determinado evento.

Otro problema inherente a NTP se refiere a la planificación de tareas: si el reloj tiene problemas, es posible que ciertas tareas no se lleguen a ejecutar, que se ejecuten varias veces, o que se ejecuten cuando no han de hacerlo; esto es especialmente peligroso para tareas de las que depende la seguridad (como los backups).

[31] Network News Transport Protocol (Protocolo para la transferencia de noticias en red)

4.9.7 TFTP

TFTP es un protocolo de transferencia de archivos (puerto 69 basado en UDP) que no proporciona ninguna seguridad. Por tanto en la mayoría de sistemas es deseable que este servicio esté desactivado.

Al utilizar este servicio en ningún momento se solicita un nombre de usuario o una clave, lo que da una idea de los graves problemas de seguridad que ofrece este servicio.

4.9.8 FTP

Un problema básico y grave de FTP (puerto 21 en TCP) es que ha sido diseñado para ofrecer la máxima velocidad en la conexión, pero no para ofrecer la seguridad; todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto claro, con lo que un atacante no tiene más que capturar todo ese tráfico y conseguir así un acceso válido al servidor.

Para solucionar este problema es conveniente dar acceso FTP a pocos usuarios bien identificados y que necesiten utilizarlo, concientizándolos de la utilidad de aplicaciones que cifren todo el tráfico de información (como SSH por ejemplo).

4.9.8.1 FTP ANÓNIMO

El servicio FTP se vuelve especialmente preocupante cuando se trata de configurar un servidor de FTP anónimo; muchos de estas máquinas situadas en universidades y empresas se convierten en servidores de imágenes pornográficas, de Warez (copias ilegales de programas comerciales). Conseguir un servidor de FTP anónimo seguro puede llegar a ser una tarea complicada.

4.9.8.2 FTP INVITADO

El otro tipo de acceso FTP es el denominado invitado (guest). La idea de este mecanismo es muy sencilla: se trata de permitir que cada usuario conecte a la máquina mediante su login y su contraseña, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo; se conectará a un entorno restringido de forma similar a lo que sucede en los accesos anónimos.

Para poder crear fácilmente entornos FTP restringidos a cada usuario, es conveniente instalar programas para este fin en la máquina servidor. Estos servidores permiten crear usuarios invitados configurando el entorno al que van a conectarse los usuarios, su estructura de directorios-archivos y sus permisos a los recursos.

4.9.9 TELNET

El protocolo TELNET (TCP, puerto 23) permite utilizar una máquina como terminal virtual de otra a través de la red, de forma que se crea un canal virtual de comunicaciones similar (pero mucho más inseguro) a utilizar una terminal físicamente conectada a un servidor.

TELNET no utiliza ningún tipo de cifrado, por lo que todo el tráfico entre equipos se realiza en texto claro. Cualquier intruso con un Sniffer puede capturar el Login y el password utilizados en una conexión otorgando a cualquiera que lea esos datos un acceso total a la máquina destino.

Es muy recomendable no utilizar TELNET para conexiones remotas, sino sustituirlo por aplicaciones equivalentes pero que utilizan cifrado para la transmisión de datos.

4.9.10 SMTP

La mala configuración del servicio SMTP[32] (puerto 25 en TCP) utilizado para transferir correo electrónico entre equipos remotos; suele ser causante del Mail Bombing y el Spam redirigido.

4.9.11 SERVIDORES WWW

Las conexiones a servidores web son sin duda las más extendidas entre usuarios de Internet.

Los problemas de seguridad relacionados con el protocolo HTTP se dividen en tres grandes grupos en función de los datos a los que pueden afectar:[33]

- **Seguridad en el servidor:** Es necesario garantizar que la información almacenada en la máquina servidora no pueda ser modificada sin autorización, que permanezca disponible y que sólo pueda ser accedida por los usuarios a los que les esté legítimamente permitido.
- **Seguridad en la red:** Cuando un usuario conecta a un servidor web se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente desde el servidor sean los mismos que se están enviando (esto es, que no sufran modificaciones de terceros).
- **Seguridad en el cliente:** Es necesario garantizar al usuario que descarga páginas de un servidor no va a perjudicar a la seguridad de su equipo. Se deben evitar Applets maliciosos, programas con virus o simples cuelgues al acceder a las páginas de la organización.

Los problemas relacionados con servidores Web suelen proceder de errores de programación en los CGIs[34] ubicados en el servidor. La capacidad del CGI para comunicarse con el resto del sistema que alberga las páginas es lo que le otorga su potencia.

---

[32] Simple Mail Transfer Protocol: Protocolo Simple de Transferencia de Correo

[33] HUERTA, Antonio Villalón. Seguridad en Unix y redes – Digital Open Publication Licence v.10 o Later 2 de Octubre 2000.

[34] *Common Gateway Interface*, una tecnología que se usa en los servidores web.

Pero también lo que causa mayores problemas de seguridad: un fallo en estos programas suele permitir a cualquier "visitante" ejecutar órdenes en el sistema.

Una medida de seguridad básica es ejecutar el demonio servidor bajo la identidad de un usuario con privilegios mínimos para que todo funcione correctamente, pero nunca como Administrador, Root o cuenta del sistema.

Para garantizar la seguridad de los datos que circulan entre un cliente y el servidor es casi obligatorio cifrar dichos datos (mediante SSL o utilizando Certificados Digitales por ejemplo).

4.10 CRIPTOLOGÍA

4.10.1 AUTENTIFICACIÓN

Se entiende por Autentificación cualquier método que permita garantizar alguna característica sobre un objeto dado. Interesa comprobar la autentificación de:

a. Un Mensaje mediante una firma: se debe garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. A este mecanismo se lo conoce como **Firma Digital** y consiste en asegurar que el mensaje **m** proviene del emisor **E** y no de otro.
b. Un Usuario mediante una contraseña: se debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta.
c. Un Dispositivo: se debe garantizar la presencia de un dispositivo válido en el sistema, por ejemplo una llave electrónica.

4.10.1.1 FIRMA DIGITAL

Una firma digital se logra mediante una Función Hash de Resumen. Esta función se encarga de obtener una "muestra única" del mensaje original. Dicha muestra es más pequeña y es muy difícil encontrar otro mensaje que tenga la misma firma. Suponiendo que B envía un mensaje m firmado a A, el procedimiento es:

a. B genera un resumen del mensaje r(m) y lo cifra con su clave privada.
b. B envía el criptograma.
c. A genera su propia copia de r(m) usando la clave pública de B asociada a la privada.
d. A compara su criptograma con el recibido y si coinciden el mensaje es auténtico.

Cabe destacar que:

1. Cualquiera que posea la clave pública de B puede constatar que el mensaje proviene realmente de B.
2. La firma digital es distinta en todos los documentos: si A firma dos documentos produce dos criptogramas distintos y; si A y B firman el mismo documento m también se producen dos criptogramas diferentes.

Las funciones Hash están basadas en que un mensaje de longitud arbitraria se transforma en un mensaje de longitud constante dividiendo el mensaje en partes iguales, aplicando la función de transformación a cada parte y sumando todos los resultados obtenidos.

Actualmente se recomienda utilizar firmas de al menos 128 bits (38 dígitos) siendo 160 bits (48 dígitos) el valor más utilizado.

4.10.2 PGP (PRETTY GOOD PRIVACY)

Este proyecto de "Seguridad Bastante Buena" pertenece a Phill Zimmerman quien decidió crearlo en 1991 "por falta de herramientas criptográficas sencillas, potentes, baratas y al alcance del usuario común[35].

Actualmente PGP es la herramienta más popular y fiable para mantener la seguridad y privacidad en las comunicaciones tanto para pequeños usuarios como para grandes empresas.

[35] http://pgp.org

4.10.2.1 FUNCIONAMIENTO DE PGP

4.10.2.1.1 ANILLOS DE CLAVES

Un anillo es una colección de claves almacenadas en un archivo. Cada usuario tiene dos anillos, uno para las claves públicas y otro para las claves privadas. Cada una de las claves, además, posee un identificador de usuario, fecha de expiración, versión de PGP y una huella digital única hexadecimal suficientemente corta que permita verificar la autenticidad de la clave.

4.10.2.1.2 CODIFICACIÓN DE MENSAJES

Los algoritmos simétricos de cifrado son más rápidos que los asimétricos. Por esta razón PGP cifra primero el mensaje empleando un algoritmo simétrico con una clave generada aleatoriamente (clave de sesión) y posteriormente codifica la clave haciendo uso de la llave pública del destinatario.

Dicha clave es extraída convenientemente del anillo de claves públicas a partir del identificador suministrado por el usuario.

Nótese que para que el mensaje pueda ser leído por múltiples destinatarios basta con que se incluya en la cabecera cada una de las claves públicas correspondientes.

4.10.2.1.3 DECODIFICACIÓN DE MENSAJES

Cuando se trata de decodificar el mensaje, PGP simplemente busca en la cabecera las claves públicas con las que está codificado, pide una contraseña para abrir el anillo de claves privadas y comprueba si se tiene una clave que permita decodificar el mensaje.

Nótese que siempre que se quiere hacer uso de una clave privada, habrá que suministrar la contraseña correspondiente, por lo que si este anillo quedara comprometido, el atacante tendría que averiguar dicha contraseña para descifrar los mensajes.

4.10.2.1.4 COMPRESIÓN DE ARCHIVOS

PGP generalmente comprime el texto plano antes de encriptar el mensaje (y lo descomprime después de desencriptarlo) para disminuir el tiempo de cifrado, de transmisión y de alguna manera fortalecer la seguridad del cifrado ante el criptoanálisis que explotan las redundancias del texto plano.

PGP utiliza rutinas de compresión de dominio público creadas por Gaily-Adler-Wales (basadas en los algoritmos de Liv-Zemple) funcionalmente semejantes a las utilizadas en los softwares comerciales de este tipo.

4.10.2.1.5 Algoritmos Utilizados por PGP

Las diferentes versiones de PGP han ido adoptando diferentes combinación de algoritmos de signatura y cifrado eligiendo entre los estudiados. Las asignaturas se realizan mediante MD5, SHA-1 y/o RIPE-MD6. Los algoritmos simétricos utilizados pueden ser IDEA, CAST y TDES y los asimétricos RSA y El Gamal.

CAPITULO V

ESTRATEGIAS PARA LA SEGURIDAD LOGICA

Es importante recalcar que la mayoría de los daños que puede sufrir cualquier organización no será sobre los medios físicos sino contra información almacenada y procesada.

Después de investigar y analizar la investigación cualitativa nos percatamos de que las amenazas y mecanismos a los cuales está expuesta en mayor grado la seguridad lógica de la organización se deriva de dos ámbitos:

Internos: Insiders y ex empleados, debido a que estos son personal que conocen los puntos fuertes y débiles del sistema, y estos pueden ser más directos y difíciles de detectar; para el caso de los insiders estos pueden ocasionar daño al sistema por accidente o intencionalmente, para el caso de los ex empleados estos pueden ocasionar daño debido a que fueron despedidos y no quedaron conformes, es mas intencional.

Externos: Hackers, Crackers, Samurai y Creadores de Virus, estos son personajes a los cuales hay que tenerle respeto debido a que como ya mencionamos anteriormente son capaces de vulnerar e introducirse a los sistemas y causar daños irreversibles e irreparables.

Visto lo anterior *las estrategias y mecanismos* que desde nuestro punto de vista proponemos son las siguientes:

5.1 MEDIDAS DE SEGURIDAD PARA EQUIPO INFORMATICO

Que solo el personal autorizado por la organización sea el único responsable de instalar el software (SW) básico para el uso de las computadoras de escritorio y portátiles. Solo en el caso de requerir de la instalación de alguna licencia de SW diferente a la entregada originalmente, deberá solicitarse a la organización con la justificación correspondiente para que determine su procedencia. En caso se que la licencia deba ser instalada por un tercero, esta deberá estar supervisada por el personal autorizado por la organización.

Los equipos informáticos cuenten con un sello de seguridad proporcionado por la organización el cual no podrá ser removido por ninguna persona ajena al personal autorizado.

Los equipos no tengan habilitados los puertos de comunicación (usb, paralelo, serial), los dispositivos de almacenamiento removible ni los dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo) a excepción de los que hayan sido previamente autorizados por la organización.

Prohibir el uso de dispositivos de almacenamiento externo para la transmisión de información confidencial en soportes electrónicos, mediante traslado físico.

El acceso a equipos informáticos con el propósito de realizar labores de mantenimiento y correctivo o soporte técnico, sea exclusivo para el personal autorizado por la organización y/o proveedor externo contratado para tal efecto.

5.2 SEGURIDAD LOGICA

5.2.1 SEGURIDAD EN EL SERVICIO DE INTERNET

No permitir el trafico de correo electrónico “SMTP” directo, el trafico de correo se realizara exclusivamente por medio del servidor central de correo electrónico interno, lo cual evitara que ser propaguen virus que intenten mandarse así mismo por este medio.

Prohibir ejecutar programas encargados de analizar el trafico de red de la organización, sistemas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de maquinas locales o remotas, hacer uso de herramientas para el rastreo de vulnerabilidades o para obtener privilegios en equipos de computo no otorgados por la organización.

5.3 SEGURIDAD EN LOS SERVIDORES

La autenticación del acceso a los servidores o equipos de computo a nivel sistema operativo donde residan los sistemas y aplicaciones de la organización contemplan los siguientes puntos:

- Para acceder a los servidores a nivel sistema operativo se deberá realizar mediante un proceso de autenticación, el cual puede realizarse mediante los siguientes métodos: login.password, Token o Sistemas biométricos; el método empleado dependerá del nivel de seguridad requerido.
- El password o contraseña deberá contar con al menos 5 a 8 caracteres alfanuméricos.
- El acceso a servidores Windows, Linux o Unix de manera remota, se realizara por medio de un login o un password, a travez de un servicio seguro de ssh (secure shell) y para transferencia de archivos sftp (secure file transfer protocol).
- Respecto al punto anterior, no se podrá acceder por servicios inseguros como telnet, o ftp y se deberá hacer un túnel empleado VPN o ssh.
- Solo estarán disponibles los servicios de red utilizados por el servidor, dejando a los demás servicios inhabilitados. Por ejemplo para servicios web solo deberá estar disponible el servicio http y https.

5.4 SEGURIDAD EN APLICACIONES Y SISTEMAS

En la autentificación de acceso a los sistemas y aplicaciones consideramos los siguientes puntos:

- Cuando un sistema maneje contraseñas, estas deberán almacenarse cifradas en el sistema y deberán contener al menos5 caracteres alfanuméricos.
- Las cuentas de usuario de aplicaciones tendrán el nombre de usuario y un grupo especifico a la aplicación. Definiendo un identificador único para usuario y grupo, o en su defecto se determinaran los niveles de acceso a la aplicación mediante un esquema de perfiles, en donde se contaran con atributos y/o opciones por usuario para trabajar dentro de cada aplicación.

- El usuario de la(s) aplicación(es) serán los responsables de su cuenta y clave de acceso, en el entendido de que la clave es personal, confidencial e intransferible. El cifrado de las contraseñas se deberán realizar mediante algoritmos criptográficos unidireccionales, donde sea posible cifrar los datos pero no descifrarlos.

5.5 SEGURIDAD EN APLICACIONES SOBRE SERVICIO WEB

En cuanto a los sistemas que operen bajo una arquitectura Web consideramos los siguientes puntos:

- La comunicación entre clientes y el Servidor Web deberá realizarse utilizando HTTPS.
- En caso de utilizar certificados digitales, proponemos lo siguiente:
- Ser compatibles con el estándar X.509 , tener una vigencia máxima de 1 año y un tamaño mínimo de 128 bits.
- Si el sistema requiere de autentificación por parte del Cliente, adicional al certificado del servidor utilizado en el protocolo HTTPS, se deberá solicitar e instalar un certificado por cada uno de los clientes que se conecten al sistema de información.

5.6 SEGURIDAD SOBRE LA TRANSFERENCIA DE DATOS

1. La información transmitida fuera de la red de la organización deberá viajar protegida bajo esquemas seguros de cifrado, utilizando para ello protocolos como: ssh, scp, sftp.
2. Los sistemas de información no deberán utilizar protocolos que transmitan la información en texto claro, como por ejemplo: telnet o ftp en su reemplazo deberán seleccionarse protocolos seguros que soporten la transmisión de mensajes cifrados.
3. Para el intercambio de datos entre sistemas y aplicaciones en forma continua, se deberá implementar un mecanismo que soporte un algoritmo de cifrado asimétrico, con el fin de elevar el nivel de confidencialidad de sistema. Por ejemplo GPG (GNU Privacy Guard).

5.6.1 SERVICIOS DE CONFIDENCIALIDAD EN LA BASE DE DATOS

Los sistemas y aplicaciones requieren salvaguardar los datos que almacenan, para lo cual se deberá realizar el cifrado de datos:

- Empleando preferentemente algoritmos de criptografía asimétricos o en su defecto uso de algoritmos simétricos.
- O mediante el uso de herramientas de atributos que la base de datos proporcione, para realizar esta tarea.

5.7 RESPALDO DE LOS SISTEMAS Y APLICACIONES

Los sistemas y aplicaciones deberán seguir los siguientes puntos en lo que respecta a procedimientos de respaldo:

- Se deberán respaldar al menos 6 días a la semana, debiendo contener la información de los días laborales, y al menos uno de esos días, se debe hacer respaldo completo. Estos respaldos deben ejecutarse diariamente, semanalmente y mensualmente, con al menos los siguientes periodos de retención:

Respaldos diarios: 7 días.

Respaldos semanales: 1 mes.

Respaldos mensuales: 1 año.

Respaldos históricos o especiales: 5 años.

El esquema de respaldos dependerá de las necesidades de cada sistema, cumpliendo como mínimo con respaldos que en caso de contingencia permitan la restauración de no más de dos días.

- Se recomienda que el usuario de los sistemas y aplicaciones cuente con una copia de respaldo mensual o anual dependiendo de lo que considere el usuario y organización, dicho respaldo se guardara hasta la sustitución de este, esto con el objetivo de salvaguardar la información fuera del centro de datos.

- Los procedimientos para el respaldo de la información deberán estar automatizados, en este proceso debe considerarse la rotación de los medios en que se almacena la información y su ejecución durante las horas de menor carga del sistema.
- Periódicamente se debe realizar una validación de los procedimientos de restauración de la información sobre ambientes no productivos, asi como también se debe monitorear la utilización de los medios de almacenamiento extraíbles a fin de evitar desgaste.
- La información contenida en medios extraíbles deberá ser de uso exclusivo para el personal que por el desarrollo de sus funciones requiera utilizarla, no deberá estar a disposición de personas ajenas.
- Para los medios extraíbles, como cartuchos de cinta, utilizados en el respaldo de datos personales que hubieran alcanzado el final de su vida útil, estos deberán ser destruidos mediante el siguiente proceso:
    a) Transferir a otro medio los archivos que contengan la información que sea preciso conservar.
    b) Sobrescribir con un solo valor el 100% de la capacidad de almacenamiento que contengan.
    c) Realizar un nuevo formateo sobre el medio extraíble.
    d) Si es posible destruirlo físicamente.

CONCLUSIONES

CONCLUSIONES

- Cuando se diseña un sistema se lo hace pensando en su Operatividad-Funcionalidad dejando de lado la Seguridad
- Será necesario establecer una correspondencia y pertenencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.
- El profesional cuenta con la misma tecnología para la evaluación de la seguridad del bien a proteger y otras pensadas para la protección como fin. Esto hace que muchas veces, la seguridad, sea asunto de la idoneidad del profesional.
- La Seguridad Perfecta requiere un nivel de perfección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables.
- El costo en el que se incurre suele ser una insignificancia comparados con aquellos luego de producido un daño. El desconocimiento y la falta de información son el principal inconveniente cuando se evalúa la inclusión de seguridad como parte de un sistema.
- El desarrollo de software es una ciencia imperfecta; y como tal es vulnerable.

Es importante comprender que:

- La seguridad consiste en tecnología y política. Es decir que la combinación de la tecnología y su forma de utilización determina cuan seguros son los sistemas.
- El problema de la seguridad no puede ser resuelto por única vez. Es decir que constituye un viaje permanente y no un destino.
- En última instancia la seguridad es una serie de movimientos entre buenos y malos.

BIBLIOGRAFIA

1. Siyan, Karanjit Prentice-Hall 1995, Internet y seguridad en redes.
2. Oppliger, Rolf Ra-Ma 1998. Sistemas de autentificación para la seguridad en redes.
3. Nombela, Juan José Paraninfo. 1997, Seguridad Informática.
4. Morant Ramón, José Luis, 1994. Centro de Estudios Ramón Areces. Seguridad y protección de la información.
5. González, Guillermo. RA-MA, 1990. El libro de los virus y de la seguridad informática.
6. CODA. CODA, 1992. Seguridad informática.
7. Black Uylees, 1999. Redes de computadoras, protocolos, normas e interfaces. Ed. Rama, México.
8. Fine, Leonard H, 1990. Seguridad de centros de cómputo, políticas y procedimientos. Editorial Trillas, México.
9. Tanembaum, Andrew, 2003. Redes de computadora. Editorial Prentice-Hall, México.
10. Aldegani, Gustavo M, 1997. Seguridad Informática. Ediciones M.P. Argentina.
11. Bello, Agustín F, (Tesis) 1997. Auditoria o sistemas en desarrollo y operación. Colegio de Posgraduados, México.
12. Huerta, Antonio. Seguridad en Unix y redes (Versión 1.2), cap. 16.
13. Lucena, Manuel José. Criptografía y seguridad en Computadoras, 2ª Edición. Departamento de Informática, Escuela Politécnica Superior.
14. Méndez, Andrés, 2000. Segunda recopilación de arroba, Manual de hacker, arroba.
15. Rodríguez, Julio Ángel, 1995. Seguridad de la información en sistemas de cómputo. Editorial S.A. de C.V.
16. Gómez Vieites Álvaro, Enciclopedia de la seguridad informática. 1era edición. México D.F. Alfaomega Grupo Editorial S.A. de C.V., 2007.

CYBERBIBLIOGRAFIAS

1. Anonimous, 2006. Historia del centro de cómputo, consultado en línea. http://www.chapingo .mx/ccul.
2. Idy, 2006. Vulnerabilidad en redes, consultado en línea. http://www.idg.es/ccomunicaciones/impart.asp.
3. Hcolima, 2007. Encriptamiento, documento consultado en línea. http://www.itcolima.edu.mx/profesores/tutoriales/sistemasdistribuidos.
4. Lucas, 2007. Seguridad informática, documento consultado en línea. http://www.es.tldp.org/ManualesLucas/segunix-2-1-html/node.htm.
5. Wikimedia, 2007. Documento sobre definiciones informáticas, consultado en línea. http://www.es.wikimedia.org/wiki/informatica.
6. http://www.cuentame.inegi.gob.mx/museo/cerquita/redes/seguridad/intro.htm
7. http://www.neoteo.com/agujero-de-seguridad-en-uac-de-windows-7-y-14695.neo