UNIVERSIDAD AMERICANA

Redes de comunicación

Recopilación de teoría referente a la materia

Ing. Luis Müller

2011

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

Unidad I – conceptos basicos

Conceptos de seguridad. Amenazas de seguridad. Modelos de seguridad. Ejemplos de casos en el mundo real. Posibles ataques. Seguridad en redes.

Seguridad en Redes de Computadores/Ataques contra las redes

Durante los primeros años de internet, los ataques a sistemas informáticos requerían pocos conocimientos técnicos. Por un lado, los ataques realizados desde el interior de la red se basaban en la alteración de permisos para modificar la información del sistema. Por el contrario, los ataques externos se producían gracias al conocimiento de las contraseñas necesarias para acceder a los equipos de la red.

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

En la mayor parte de la bibliografía relacionada con la seguridad en redes informáticas podemos encontrar clasificadas las tres generaciones de ataques siguientes:

Primera generación: ataques físicos. Encontramos aquí ataques que se centran en componentes electrónicos, como podrían ser los propios ordenadores, los cables o los dispositivos de red. Actualmente se conocen soluciones para estos ataques, utilizando protocolos distribuidos y de redundancia para conseguir una tolerancia a fallos aceptable.

Segunda generación: ataques sintácticos. Se trata de ataques contra la lógica operativa de los ordenadores y las redes, que quieren explotar vulnerabilidades existentes en el software, algoritmos de cifrado y en protocolos. Aunque no existen

soluciones globales para contrarrestar de forma eficiente estos ataques, podemos encontrar soluciones cada vez más eficaces.

Tercera generación: ataques semánticos. Finalmente, podemos hablar de aquellos ataques que se aprovechan de la confianza de los usuarios en la información. Este tipo de ataques pueden ir desde la colocación de información falsa en boletines informativos y correos electrónicos hasta la modificación del contenido de los datos en servicios de confianza, como, por ejemplo, la manipulación de bases de datos con información pública, sistemas de información bursátil, sistemas de control de tráfico aéreo, etc.

Seguridad informática

La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Objetivos de la seguridad informática

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

- **La información contenida**

  Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los

criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

- **La infraestructura computacional**

  Una parte fundamental para el almacenamiento y gestión de la información, asi como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- **Los usuarios**

  Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general. y como principal contribuyente al uso de programas realizados por programadores

Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la

descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
- Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o *Script boy*, viruxer, etc.).
- Un siniestro (robo, incendio, inundación): una mala manipulación o una malintención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

Tipos de amenaza

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. Basado en esto podemos decir que existen 2 tipos de amenazas:

- **Amenazas internas**: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

-Los usuarios conocen la red y saben cómo es su funcionamiento.

-Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

-Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

- **Amenazas externas**: Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

La amenaza informática del futuro

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los significados de la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

- Se puede afirmar que “la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas”.
- Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información

En este sentido, las amenazas informáticas que vienen en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de

que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

- “La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas”, La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital”.

Para no ser presa de esta nueva ola de ataques más sutiles, Se recomienda:

- Mantener las soluciones activadas y actualizadas.
- Evitar realizar operaciones comerciales en computadoras de uso público.
- Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.

Tipos de Virus

Los virus se pueden clasificar de la siguiente forma:

Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser

ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Virus de sobreescritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

Virus de boot o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador.Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un ordenador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro.

Virus de macro

El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc. Las macros son micro-programas asociados a un fichero, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.

Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Virus cifrados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

Virus polimórficos

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

Virus multipartites

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Virus de Fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema.Los virus que atacan a este elemento son especialmente peligrosos, ya

que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.

Análisis de riesgos

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: *"lo que no está permitido debe estar prohibido"* y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

- Planes para reducir los riesgos.

Análisis de impacto al negocio

El reto es asignar estratégicamente los recursos para equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los Valores para el sistema se pueden distinguir: Confidencialidad de la información, la Integridad (aplicaciones e información) y finalmente la Disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor Web público pueden poseer los requisitos de confidencialidad de baja (ya que toda la información es pública),pero de alta disponibilidad y los requisitos de integridad. En contraste, un sistema de planificación de recursos empresariales (ERP),sistema puede poseer alta puntaje

en los tres variables. Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

Puesta en marcha de una política de seguridad

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Ej: En España la Ley Orgánica de Protección de Datos o también llamada LOPD y su normativa de desarrollo.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

Técnicas para asegurar el sistema

- Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red. Zona desmilitarizada
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.
- Sistema de Respaldo Remoto. Servicio de backup remoto

Respaldo de Información

La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup). Es vital para las empresas elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

Continuo

> El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.

Seguro

Muchos softwares de respaldo incluyen cifrado de datos (128-448 bits), lo cual debe ser hecho localmente en el equipo antes del envío de la información.

Remoto

Los datos deben quedar alojados en dependencias alejadas de la empresa.

Mantención de versiones anteriores de los datos

Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

Hoy en día los sistemas de respaldo de información online (Servicio de backup remoto) están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información sin tener que estar preocupados de aumentar su dotación física de servidores y sistemas de almacenamiento.

Consideraciones de software

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Existe un software que es conocido por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades pero permitiendo una seguridad extra.

Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

Algunas afirmaciones erróneas comunes acerca de la seguridad

Mi sistema no es importante para un cracker

Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues ¿quién va a querer obtener información mía?. Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.

Estoy protegido pues no abro archivos que no conozco

Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.

Como tengo antivirus estoy protegido

En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.

Como dispongo de un firewall no me contagio

Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el spoofing.

Tengo un servidor web cuyo sistema operativo es un Unix actualizado a la fecha

Puede que este protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etc.) está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra una shell y por ende ejecutar comandos en el unix.

Organismos oficiales de seguridad informática

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el **CERT/CC** (*Computer Emergency Response Team Coordination Center*) del *SEI* (Software Engineering Institute) de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

Tipos de Ataques

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, etc. 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 "agujeros" en el diseño, configuración y operación de los sistemas.

- **Ingeniería Social**
- **Ingeniería Social Inversa**
- **Trashing (Cartoneo)**
- **Ataques de Monitorización**
- **Ataques de Autenticación**
- **Denial of Service (DoS)**
- **Ataques de Modificación - Daño**

Entre ellos:

Ataques de intromisión: Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

Ataque de espionaje en líneas: Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.

Ataque de intercepción: Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una red.

Ataque de modificación: Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad del los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.).

Ataque de denegación de servicio : Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

Ataque de suplantación: Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha

puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Ingeniería social: Con este tipo de práctica, el intruso puede obtener horarios de trabajo, claves de acceso, nombres de empleados e infiltrarse indirectamente en la organización, empresa y/o inclusive en nuestras casas. Puede obtener información con una simple plática, siendo amigables y mintiendo con alguien que trabaja en la empresa y/o organización. También a través de una llama telefónica haciéndose pasar por un empleado que pide soporte técnico a la empresa que le proporciona dicho servicio, o también haciéndose pasar por algún agente bancario y/o de seguros que trata de vender o prestar su servicio y todo esto hecho vía telefónica. Es también común recibir un correo electrónico informado que se ha ganado un premio y se requieren algunos datos para enviar el supuesto premio a al domicilio.

¿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. Filtrar el tráfico IP Spoof.
6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, **la capacitación continua del usuario**.