

Universidad Tecnológica de Panamá

Facultad de Ingeniería de Sistemas Computacionales

Departamento de Programación de Computadoras

Asignatura

Seguridad en los Sistemas de Información

Capítulo I

Introducción a la Seguridad

Prof. Isabel Leguías

2019

Objetivos:

- Definir el término seguridad y otros conceptos relacionados con este.
- Describir los diversos tipos de servicios de seguridad.
- Describir los diversos tipos de atacantes y amenazas de seguridad informática.

Introducción

En la actualidad, las organizaciones son cada vez más dependientes de plataformas digitales donde desarrollan los procesos de negocios y al mismo tiempo sus sistemas informáticos están conectados a la Internet, por lo cual cualquier problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones del negocio en las organizaciones.

La falta de medidas de seguridad en los sistemas es un problema que está en crecimiento. Los ataques a las organizaciones ocurren y evolucionan al mismo ritmo que las tecnologías expande sus servicios para agilizar las operaciones de la organización. Basta con observar el panorama en las tendencias en seguridad para conocer los distintos ataques que se dan a diario sobre todo tipo de organizaciones en todas partes del mundo.

Los ciberdelincuentes logran irrumpir en sistemas de información sin mayor dificultad para descubrir y explorar sus vulnerabilidades cada año. Sin embargo, hay estudios que revelan que muchos de los ataques consumados no fueron demasiados sofisticados; sino todo lo contrario se ejecutaron por medio de técnicas de baja complejidad explotando vulnerabilidades conocidas.

La propia complejidad de la red es otra dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “Hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las Redes.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la seguridad.

1.1 Conceptos de seguridad

En la actualidad, la seguridad de la información ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las organizaciones a nivel mundial.

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 la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

1.1.1 Consideraciones de seguridad

El Porqué de la Seguridad

Ya no se puede decir que Internet sea un fenómeno en expansión, porque Internet es una realidad en las comunicaciones actuales. La “red de redes” interconecta hoy día a prácticamente la totalidad de la población mundial, permitiendo la compartición de información a nivel global.

Esto no es todo, porque las posibilidades de Internet se extienden más allá de la simple difusión de información. Internet permite la interactividad entre usuarios, y ahí es donde radica el principal problema de seguridad.

Internet no creció con la seguridad en mente, y por tanto no incorpora ningún mecanismo de seguridad en su estructura básica, por lo que todos los servicios que se integran en Internet sufren de esas debilidades básicas, y de otras “proporcionadas” por los propios servicios, que normalmente hacen poco o ningún hincapié en los posibles fallos y “agujeros” que pueda tener. Por tanto, cuanto más usuarios se conecten a la Red y más servicios se hacen disponibles, más necesario es añadirle mecanismos de seguridad a Internet, pero para clarificar esta necesidad, hay que contestar a tres preguntas básicas:

- 1.-Que proteger
- 2.-De quien protegerlo
- 3.- Como protegerlo

Que Proteger

Es evidente que la seguridad no tendría sentido si no hubiese nada que proteger, podríamos dejar todos los agujeros y no preocuparnos de nada, pero la lógica nos dice que esto no es así. A continuación, vamos a detallar de forma exhaustiva todo lo que necesita ser protegido:

- **Datos:** La información puede ser robada, destruida o modificada, y cualquiera de los tres casos es igual de peligroso:

Robo: A una empresa puede hacerle muchísimo daño que le roben información confidencial, porque los casos de espionaje industrial por la red son cada vez más frecuentes. Por ejemplo, en un ataque realizado a Microsoft, se rumoreaba que podían haber robado los códigos fuente de Windows™ y Office™, posiblemente la posesión más preciada de una empresa de Software. Por tanto, será necesario proteger la información confidencial de las empresas y usuarios, para que no caiga en “malas manos”.

Destrucción: Otro de los desastres posibles con los datos es la destrucción de estos. Puede ser desastroso que por un descuido toda la información valiosa sea destruida, y se pierda el trabajo realizado durante mucho tiempo, o incluso que desaparezca información necesaria para el funcionamiento interno de la empresa (lista de clientes, facturación, nóminas, etc...). Incluso en el caso de que se almacenen copias de seguridad de los datos, la destrucción de estos supone una interrupción de la producción mientras se restauran los mismos, con la posible aparición de problemas derivados del hecho de restaurar unos datos “antiguos” (dependiendo de la naturaleza de los datos se pueden perder las últimas modificaciones, teniendo que buscar el punto exacto de actualización).

Modificación: Posiblemente el peor de los riesgos es el de modificación de los datos. Es el ataque más sutil de todos y puede causar grandes daños a la infraestructura de una empresa. Se podrían modificar desde los planos de un proyecto por parte de una empresa, hasta el código fuente de un software de próxima aparición. En cualquier caso, si se descubre a tiempo la intrusión (cosa que es más complicada que en el caso de la destrucción de datos) requiere una revisión completa de los datos, primero para averiguar la fuente del cambio, y luego para corregirlo. Esto suele requerir gran cantidad de tiempo, lo que provoca un retraso significativo en la normal evolución de la empresa, con la pérdida económica asociada. Muchísimo peor es no advertir la modificación, lo que puede producir un desastre que acabe con una empresa.

- Programas: Al igual que los datos, los programas de computador deben ser protegidos, entre otras cosas porque son una forma de acceso a los datos. Los programas manejan la información y acceden al sistema, con lo cual son una herramienta perfecta para conseguir los objetivos del “pirata informático”. Son conocidas por todas las debilidades que presenta el Internet Explorer, que permite, por ejemplo, que se ejecuten instrucciones en el computador poniendo la URL apropiada.

Entre las herramientas de Software más utilizadas están las Back Orifice (Puertas Traseras), que esperan, suplantando a otra aplicación (Notepad, PaintBrush...) a que se ejecuten, momento en el que se instalan en el computador y permiten el acceso remoto al hacker, pudiendo este controlar el PC como si estuviese presente.

- Hardware: Otras veces, el hacker pretende usar los recursos disponibles, más que los propios datos, por ejemplo, para iniciar un ataque desde una máquina que no es suya, y así permanecer en el anonimato. Otras veces utiliza las máquinas como servidores ilegales (por ejemplo, de FTP) o utiliza los recursos para acceder a servicios a los que normalmente no accedería.

Este es el principal riesgo para los usuarios finales, porque los datos que pueda perder un usuario son insignificantes en la mayoría de los casos, pero que tu computador aparezca como el origen de un ataque a una corporación importante puede acarrear grandes problemas. Además, determinadas páginas “poco recomendables” (normalmente de contenido pornográfico) intentan instalar (sin permiso) conexiones de Red distintas de la que tenga contratada el usuario (normalmente un 906), para que sin saberlo este haciendo uso de ese servidor, y, por tanto, facturando llamadas.

- Imagen: No hay nada que produzca más desconfianza, que una empresa que ha sido atacada o que ha sido usada como soporte para un ataque a una tercera persona. Crea una apariencia de dejadez que no beneficia a la empresa. Por tanto, es importante que una empresa mantenga una buena seguridad, máxime si esta empresa es de Software. Además, cuando se encuentra una brecha de seguridad, esta es inmediatamente conocida en la red, lo cual provoca que los ataques se multipliquen a menos que la brecha sea rápidamente contenida.



De Quien Protegerlo

Hay 2 tipos de atacantes de los que preocuparse: Los hackers profesionales y los llamados Tiny Hackers. Los primeros son, afortunadamente, una minoría, y son los que se encargan de buscar debilidades y de crear aplicaciones capaces de aprovechar estas vulnerabilidades. Luego, estos programas de crack son distribuidos por la red y usados por una gran cantidad de Tiny Hackers, que en realidad lo único que buscan es un poco de fama, o simplemente “gastar una broma”.

Los hackers que de verdad preocupan son los primeros, ya que son realmente capaces de conseguir sus fines, si se lo proponen. La única forma eficaz de protegerse de ellos es conseguir que sea tan difícil atacar la red que no les merezca la pena emplear tanto tiempo. Esto es tanto más difícil cuanto más importante es la red que proteger.

Los otros hackers son sobre todo una molestia, porque al utilizar los programas que todo el mundo conoce son más fáciles de parar. Es relativamente sencillo crear defensas para protegerse de ellos, por eso las víctimas de estos “piratas” suelen ser usuarios desprevenidos, o redes no lo suficientemente protegidas.

Los ataques pueden clasificarse en 3 tipos genéricos:

-  Desmantelamiento de sistemas: Suelen ser ataques de Denial of Service. Estos ataques tienen como fin colapsar una o más máquinas, haciendo que se “cuelguen”, e incluso provocando la pérdida de datos (esto último dependiendo del sistema operativo). La forma más sencilla de provocarlo es inundando de peticiones a la/las máquinas, hasta que se acaba la memoria y se cuelga.
-  Robo de datos: La manera más normal de atacar para robar datos es conseguir una combinación de login/password de algún usuario (cuantos más privilegios tenga ese usuario, mejor). Esto se puede conseguir probando combinaciones de password

contra algún login conocido (o contra todos), empezando por las combinaciones más típicas y luego probando todas las posibles (ataques de fuerza bruta). Otra forma de conseguir un login/password es mediante un sniffer, un programa que captura todos los datos que pasen por la red. Muchas aplicaciones mandan información por la red sin encriptar (como Telnet) y puede ser analizada por un atacante para encontrar una identificación con la que acceder al sistema.

✚ **Intrusión:** Estos ataques consiguen que el hacker tenga acceso remoto a otra máquina, y por tanto puede usar los recursos de esta. Normalmente se utilizan estas máquinas para lanzar ataques contra otras de una forma “camuflada”, y sin un riesgo claro para el atacante.

En cualquier caso, todos los ataques suelen ir acompañados de un trabajo de “limpiado de huellas”, ya que el hacker debe cubrir su ataque para no ser descubierto. En general, el hacker suele hacer “spoofing”, que consiste en utilizar una dirección IP de origen que no es la suya, para así cubrirse él. Otra de las técnicas es lanzar el ataque de forma remota desde una máquina que haya sido atacada previamente lo cual también cubre al atacante real. Además, se suele completar la “limpieza” camuflando las actividades en el ataque, mediante una modificación de los archivos de logging, de tal forma que no aparezca ningún rastro del ataque.

Por eso, es muy importante a la hora de proteger una red que se tenga un buen sistema de informes, principalmente para que un ataque no pueda pasar desapercibido y para que se pueda rastrear al atacante. Este sistema debe ser exhaustivo, de tal forma que recoja la información de todo lo que pase en el sistema, y además debe ser difícil de modificar, para que no se pueda manipular fácilmente.

Como Protegerlo

No existe una forma genérica para proteger una red (o un único computador) de cualquier ataque. Hay muchos factores a tener en cuenta, desde la importancia de los datos a proteger (no es lo mismo proteger una pequeña red que solo se usa para tener una forma de inventario muy rápida, que proteger una red gubernamental), hasta el presupuesto disponible para seguridad. Se colocan equipos conocidos como firewalls (cortafuegos) que son los que proporcionan la seguridad a la red, mediante un análisis del tráfico, permitiendo unas cosas y denegando otras (en función de la configuración elegida).

Como ya hemos comentado antes, es importante plantearse la importancia de lo que se va a proteger, para hacerse una idea de los esfuerzos que están dispuestos a hacer los hackers para conseguir atacar la red. Incluso es necesario plantearse la naturaleza del servicio que se ofrece, porque determinadas empresas son susceptibles de ser atacadas por motivos ajenos a la información que posea (Microsoft, servidores de Web como Yahoo, Telefónica...).

Una vez se tiene claro el nivel de seguridad que va a ser necesario (y siempre con la restricción económica en mente), se debe decidir qué tipo de topología se va a adoptar en la red. No es lo mismo una pequeña red, donde se pueden concentrar los esfuerzos en proteger un número pequeño de máquinas, que una gran red separada en múltiples segmentos, con distintos privilegios y necesidades, donde será necesario distribuir la responsabilidad de la seguridad (poner varios firewalls), y prestar más atención a cada segmento. Existen muchos tipos de Topologías de seguridad más o menos “conocidas” por todos, y que están recomendadas para distintos casos, pero aun así es necesario un estudio pormenorizado, entre otras cosas porque las redes suelen hacerse primero y se “aseguran” después, con lo que las opciones suelen restringirse mucho. Las configuraciones más normales consisten en un firewall en “punta de lanza” (como primer obstáculo) y luego otros firewalls en cada segmento separado, añadiendo más seguridad a cada subred, dependiendo en la naturaleza de estas.

Existe un tipo “especial” de segmento, conocido como DMZ (De-Militarized Zone), donde se suelen colocar los equipos de “riesgo”, como los servidores que deben ser accesibles desde la zona Internet (servidores de www, correo, IRC...). Es una zona donde hay que permitir demasiadas cosas (conexiones que empiezan en el exterior...), y no es recomendable que conviva con otros equipos que no necesitan tantos riesgos. Esta es la configuración más típica, con un firewall al que se conecta la subred segura, el DMZ e Internet (o el acceso externo), y se crean distintas políticas para cada acceso (Internet → Interno, DMZ → Interno, Interno → Externo...). Además, se puede añadir un servidor Proxy (de

Web, de Telnet, de FTP...) para ofrecer distintos servicios con un nivel de seguridad mayor, ya que un Proxy analiza el tráfico de forma más detallista que un filtro, que solo analiza tráfico como mucho a nivel de direcciones, puertos y protocolo de nivel 4.

Una vez se tiene la topología a implementar, se pasa a analizar las necesidades de cada segmento, en función de las tareas que tenga que realizar. La política habitual es prohibir todo el tráfico que no se permita explícitamente, y solo se permite el tráfico que sea necesario. Esto requiere un conocimiento básico de Redes, para poder implementar las reglas que permiten el acceso a los servicios que requiera cada segmento, cosa que no ocurre con los proxies, ya que son totalmente automáticos, pero no existen proxies para todos los servicios, por lo que dependiendo del tipo de red (de usuarios de Internet o de Investigación) puede ser suficiente con un proxy (que implemente todos los servicios) o puede ser necesario un filtro “convencional”, en el que se configure manualmente el servicio.

Además, es necesario conocer los riesgos asociados a cada servicio que se permita en la red, para así añadir la seguridad que sea necesaria, bien en el propio firewall, o bien en los equipos finales. Puede ser necesario añadir un sistema de detección de intrusos para que monitorice el tráfico en busca de patrones conocidos de ataque, dependiendo de los servicios que se permitan. Se explicarán los riesgos de cada servicio en el próximo capítulo.

Otro de los factores a tener en cuenta es que la mayoría de los ataques comienzan desde dentro de la propia subred, bien por malicia de un usuario o bien por desconocimiento o despiste de un neófito. Por eso es muy importante concienciar a todo el mundo de las cosas que se pueden y se deben hacer, y de cuales no (no ejecutar archivos descargados de páginas de poca confianza, vigilar los attachments de los mails...), estableciendo unas políticas de seguridad para los usuarios (usuarios con distintos privilegios en función de su cargo y de sus conocimientos en informática). También sería recomendable un control de login/password, para evitar combinaciones especialmente débiles (basadas en palabras de diccionario).

Por tanto, también será importante añadir seguridad en los equipos finales, principalmente en los servidores, de los que depende gran parte del funcionamiento de una subred. Entre los dispositivos de seguridad más normales están los antivirus (preferiblemente con detección de troyanos) y los llamados “Personal Firewalls” (o Desktop Firewalls), que cumplen una función similar a un firewall estándar, pero para un equipo final (que no tiene que hacer routing). Así, podemos añadir un nivel de restricción superior que el que le corresponda por segmento de red, ya que por ejemplo desde un servidor de NFS solo será necesario que se permita el acceso NFS y ninguno más (nadie va a navegar Web desde allí), a pesar de que el firewall de ese segmento permita el tráfico red.

Por último, no se recomienda la instalación de servidores en el/los firewalls de routing, porque se pueden crear agujeros de seguridad que pongan en peligro a toda la red. Además, en la mayoría de las configuraciones, el Firewall es un “cuello de botella”, ya que actúa como router externo, y si se le añaden servicios, aumentara su tiempo de respuesta y hará que la Red funcione más lenta.

1.1.2 Definiciones

Dado que se está tratando con conceptos que pueden tener múltiples interpretaciones, se hace necesario acordar ciertos significados específicos. Por tanto, hemos recurrido a algunas definiciones, todas ellas extraídas del diccionario Espasa Calpe.

Seguridad: es “calidad de seguro”, y, seguro está definido como “libre de riesgo”. Otra definición, es estar libre de peligro, a salvo; libre del miedo o ansiedad.

En cuanto a la seguridad de la información, de acuerdo con el diccionario en línea Merriam-Webster (que se encuentra <http://www.m-w.com/>), define la información como:

Conocimiento obtenido a partir de la investigación, el estudio o instrucción, inteligencia, noticias, hechos, datos, una señal o carácter (como en un sistema de comunicación o computadora) representando datos, algo (como un mensaje, datos experimentales o una imagen) que justifique el cambio en una construcción (como un plan o una teoría) que representa la experiencia física o mental u otra construcción.

Otra definición Información: es “acción y efecto de informar”.



Informar: es “dar noticia de una cosa”.

La **seguridad informática** consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Seguridad en Redes: Es la necesidad de tener una comunicación segura, además, mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin.

Si trabajamos en definir Seguridad en Redes con los elementos que conocemos, podemos llegar a una definición más acertada:



Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Si unimos la definición de seguridad e información para obtener la

Seguridad de la información:

Medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimiento, hechos, datos o capacidades. (Tomado del libro Maiwald)

INFOSEC Glossary 2000: “**Seguridad de los Sistemas de Información** consiste en la protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas.”

Sistema de Seguridad: Es un conjunto de elementos que permiten al usuario realizar ciertas operaciones en función del nivel de responsabilidad que le ha sido asignado. Este nivel de responsabilidad depende del puesto que ocupe el usuario del sistema. El sistema ha de tratar de reducir los puntos por donde se puede producir un ataque y los que no se puedan eliminar tienen que ser controlados para evitar el ataque.

La seguridad por sí sola no puede garantizar la protección, por lo cual se hace necesario tener los preventivos para proteger tanto la información como sus capacidades.

¿Por qué es necesaria?



La seguridad es necesaria para evitar que los intrusos puedan obtener información sobre las personas o sobre las empresas para poder utilizarla a favor suyo y en perjuicio de los demás.

Es necesaria para evitar la suplantación de una persona y que se la culpe a ésta de la fechoría hecha por el intruso que ha sustituido a esa persona.

Es necesaria para poder evitar que un fallo en el sistema producido por un usuario perjudique al resto de usuarios o para evitar que el usuario emplee Internet para perder el tiempo en horas de trabajo.

La seguridad es necesaria para evitar el robo de los passwords, la alteración o robo de archivos, la introducción de virus o troyanos y para evitar que nuestro computador sea utilizado para realizar un ataque a otro.

1.1.3 Privacidad en la red

Las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna organización podría sobrevivir. Por tal razón, es necesario que las organizaciones *mantengan sus servidores, datos e instalaciones lejos de los ciberdelinquentes*.

La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos hackers aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

Definición de privacidad en redes

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.).

Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (servidores, teléfonos, ordenadores personales, teléfonos móviles, etc.).

Requisitos para mantener la privacidad de las redes

Las redes deben cumplir los siguientes requisitos o características para mantener su privacidad y poder ser más robustas ante las posibilidades de intrusión.

1. **Disponibilidad:** significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones de la empresa.
2. **Autenticación:** confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos, la autenticación de los sitios web, etc.
3. **Integridad:** confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica
4. **Confidencialidad:** protección de las comunicaciones o los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que pueden amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Amenazas o riesgos a la privacidad de las redes

Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:

1. **Intercepción de las Comunicaciones:** la comunicación puede ser interceptada y los datos copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes, por ejemplo, pinchando la línea, o controlando las transmisiones.
2. **Acceso no Autorizado a Ordenadores y Redes de Ordenadores:** el acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma mal intencionado para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques aprovechando la tendencia de la gente a utilizar contraseñas previsibles, aprovechar la tendencia de la gente a desvelar información a personas en apariencia fiable e interceptación de contraseñas.
3. **Perturbación de las Redes:** actualmente las redes se encuentran ampliamente digitalizadas y controladas por computadores, pero en el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos ordenadores. En la actualidad, los ataques más peligrosos se concretan a los puntos débiles y más vulnerables de los componentes de las redes como son sistemas operativos, encaminadores (router), conmutadores (switch), servidores de nombres de dominio (DNS), etc.
4. **Ejecución de Programas que Modifican y Destruyen los Datos:** los computadores funcionan con programas informáticos, pero lamentablemente, los programas pueden usarse también para desactivar un computador y para borrar o modificar los datos. Cuando esto ocurre en un computador que forma parte de una red, los efectos de estas alteraciones pueden tener un alcance considerable. Por ejemplo, un virus es un programa informático mal intencionado que reproduce su propio código que se adhiere, de modo que cuando se ejecuta el programa informático infectado se activa el código del virus.
5. **Declaración Falsa:** a la hora de efectuar una conexión a la red o de recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función del contexto de la comunicación. Para la red, el mayor riesgo de ataque procede de la gente que conoce el contexto. Por tal razón, las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos, como pueden ser transmitir datos confidenciales a personas no autorizadas, rechazo de un contrato, etc.
6. **Accidentes no Provocados:** numerosos problemas de seguridad se deben a accidentes Imprevistos o no provocados como: son tormentas, inundaciones, incendios, terremotos, interrupción del servicio por obras de construcción, defectos de programas y errores humanos o deficiencias de la gestión del operador, el proveedor de servicio o el usuario.

1.2 Servicios de Seguridad

Podemos definir servicio de seguridad como el servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización.

Además, de estos servicios **clásicos** que se definieron a finales de la década de los ochenta, debido a los requisitos que exigen algunos de nuevos servicios de redes que están actualmente siendo vislumbrados cabe hablar de un nuevo servicio: **anonimato**.

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger y contrarrestar los ataques. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

1.2.1 Confidencialidad: este servicio proporciona protección para evitar que los datos sean revelados, accidental o deliberadamente, a un usuario no autorizado. Mantiene el secreto de la información. Es decir, garantiza que los datos tan sólo van a ser entendibles por el destinatario o destinatarios del mensaje. Para ello, el mensaje se alternará de tal manera que aquellas personas que no sean destinatarios autorizados, aunque lo capturen, no podrán ser capaces de entender su significado.

Cuando es proporcionado, protege a los usuarios contra un ataque, muy apreciado por ciertos organismos que en teoría están para proteger al ciudadano, consistente en proteger contra el ataque de acceso, de forma indebida, a la información que por allí circula. Un ejemplo que siempre se aplica es el correo postal, en la cual como derecho cívico se le garantiza la confidencialidad en las comunicaciones convencionales mediante papel. Este involucra:

- Confidencialidad de archivos
- Confidencialidad de la información durante la transmisión (ver tabla siguiente)

- Confidencialidad del flujo de tráfico

Mecanismos de confidencialidad	Controles físicos de seguridad Control de acceso a los archivos electrónicos Encriptación de archivos
Requerimientos de archivos de confidencialidad	Identificación y autenticación Configuración apropiada del sistema computacional Se utiliza la administración apropiada de la llave de encriptación

1.2.2 Autenticación: se encarga de garantizar la autenticidad de la comunicación (entre persona o máquina) es *quien dice ser*. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

Este servicio protege contra un ataque muy fácilmente penetrable en las redes: la suplantación de identidad mediante el cual una entidad remota se hace pasar por quien no es.

Se pueden identificar dos casos distintos:

- Autenticación de origen. Cuando se garantiza que la entidad origen de la comunicación es quien dice ser.
- Autenticación de destino. Cuando se garantiza que la entidad destino de la comunicación es quien dice ser.

Puede tratarse de autenticación de entidad simple, en cuyo caso sólo uno de los participantes en la comunicación (puede ser tanto la entidad origen de los datos como el destino) está obligado a demostrar su identidad. Un ejemplo de ello puede ser el acceso a un servidor remoto que contenga una BDatos que almacene información por cuyo consumo el cliente debe pagar. Previo autorizarle el acceso y anotarle el correspondiente cargo, si el protocolo de acceso tiene implementado el servicio de autenticación, se garantiza a los gestores del servidor que el usuario que está tratando de acceder a la base de datos es la persona o entidad que proclama ser.

Podrían distinguirse en este servicio dos calidades, una de las cuales es la **Autenticación débil** y está apoyada en el uso más o menos sofisticado de palabras de paso (passwords) o de identificadores, mientras que cuando el resultado es más eficaz se le denomina **Autenticación fuerte** (strong authentication), que requiere del intercambio de mensajes, cifrados y posiblemente, de una Tercera Parte de Confianza, TTP (trusted third party). Las TTPs son agentes especializados que intervienen en las comunicaciones seguras.

1.2.3 Integridad: garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los enviados por el emisor de estos, de tal forma que puede tener garantías de que la información original no le ha sido añadida, ni modificada, ni sustraída alguna de sus partes. Es decir, el receptor de la información (o el proveedor de servicio) detectará si se ha producido o no un ataque de modificación y de refutación del mensaje, lo que le permitirá rechazar o dar por buenos los datos recibidos. Como ocurre con la confidencialidad, este servicio debe trabajar con el servicio de responsabilidad para identificar apropiadamente a los individuos. Este incluye:

- Integridad de los archivos
- Integridad de la información durante la transmisión

Cuando se trata de mensajes o datos en soporte electrónico, las posibilidades de hacer modificaciones sin dejar huellas están al alcance de cualquiera. Por ejemplo, si alguien quiera presentar ante un organismo cualquiera, como elemento probatorio, un mensaje de correo impreso en el que se respalde cualquier circunstancia favorable a quien lo presenta. Resulta evidente que si no presenta una prueba robusta (por lo general será una prueba criptográfica) de la integridad del mensaje, nadie en su sano juicio va a aceptar ese mensaje como una prueba válida (cualquiera

puede redactar e imprimir lo que le parezca oportuno y darle el formato que tendría un mensaje de correo). Por todo ello, resulta absolutamente imprescindible la provisión del servicio de integridad cuando se trata de intercambiar mensajes, con cierta garantía a través de redes de comunicaciones.

Para la integridad de datos se aplican mecanismos como por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas.

1.2.4 No repudio: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin. Se distinguen tres situaciones:

- ✚ No repudio con prueba de origen: en este caso, el receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos. En muchos casos puede bastar las garantías que el emisor introduce en el mensaje cuando aplica los mecanismos que aseguran la autenticación del origen de los datos. En otros casos pueden requerirse evidencias acerca de la relación existente entre el autor de un determinado mensaje y la entidad que procede a enviarlo a través de la red. Por ejemplo, un usuario escribe y firma una carta vejatoria hacia otra persona pero no se atreve a enviársela por correo postal. Si un tercero localiza ese escrito y lo pone en el correo, el receptor tendrá pruebas demostrables de quién es el autor de la carta, pero no de que además de escribirla ha sido él quien ha tomado la decisión ofensiva de enviársela.
- ✚ No repudio con prueba de envío: el receptor o el emisor del mensaje adquieren una prueba, demostrable ante terceros, de la fecha y hora en que el mensaje fue enviado. Este servicio trata de emular al que frecuentemente presta el Servicio Postal cuando al entregar una carta certificada en la estafeta se solicita que una copia del documento que se quiere enviar sea sellada con una marca de tiempo precisa, de tal manera que pueda servir posteriormente como prueba ante determinados actos administrativos que quieren que, por ejemplo, una solicitud sea entregada antes de una fecha concreta bien en el registro de entrada de la oficina de destino o bien en una dependencia de correos. (dependiendo de qué entidad reciba la prueba, se puede desdoblar en dos este servicio).
- ✚ No repudio con prueba de entrega: el emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado. Continuando con el ejemplo del correo, este servicio equivaldría al envío de cartas con acuse de recibo, una cartulina que sirve de evidencia y justificación de que la carta ha llegado a su destinatario.

En estos dos últimos ejemplos, el correo se comporta como una entidad intermediaria entre el emisor y el receptor, lo que traducido al mundo de las redes significa que para implantar ese servicio es necesaria alguna entidad que actúe como Tercera Parte de Confianza (TTP). Esto equivale a decir que para que este servicio pueda ser provisto es necesario que exista, en alguna medida, una infraestructura de seguridad que haga de garante y proporcione las evidencias exigidas.

Esta es la causa por la que el servicio de No Repudio es más difícil de implantar que la terna autenticación-confidencialidad-integridad que, como antes dijimos, pueden implantarse (en su versión más simplista) solamente en la entidad emisora y en la entidad receptora son el concurso de ninguna TTP intermediaria. No obstante, esta mayor dificultad, no es necesario poner mucho énfasis para trasladar la convicción de lo imprescindible que resulta la implantación de servicios de No Repudio si lo que se pretende es que, dentro de la Sociedad de la Información, la mayoría de las comunicaciones que convencionalmente han venido desenvolviéndose mediante el intercambio de documentos en papel se vean sustituidas por transferencias de documentos digitales a través de redes telemáticas.

Un ejemplo de aplicación que requiera el no repudio puede ser el simple correo electrónico. Al mandar mensajes de correo, si estos poseen información importante (como la autorización para realizar una compra, asignar tareas en una empresa, etc.) se puede requerir algo que indique que el usuario en verdad ha mandado el mensaje y luego no lo pueda negar (no repudio de origen) y que indique además que el usuario receptor del mensaje en verdad lo ha recibido.

Control de acceso: sirve para evitar el uso no autorizado de los recursos de la red. Limita y controla el acceso a sistemas host y aplicaciones por medio de enlaces de comunicaciones. Para conseguirlo, cualquier entidad que intente acceder debe antes ser identificado o autenticado, de forma que los derechos de acceso puedan adaptarse de manera individual. Puede ser acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación. De forma resumida, podríamos decir que este servicio permite especificar *quién puede hacer qué*, es decir, qué usuarios pueden hacer determinadas operaciones.

Realmente este es un servicio que ya hace mucho tiempo se viene aplicando en las redes para el control de recursos.

En las redes de comunicaciones se puede presentar la necesidad de disponer de un servicio de control de acceso en dos situaciones distintas. Estes son:

- a. El acceso remoto a servidores de todo tipo como bases de datos, impresoras, servidores de correo, etc. El usuario accede regularmente bajo una arquitectura cliente-servidor y, tras identificarse, los mecanismos en que se apoya el servicio determinan a qué partes del servicio se le concede acceso.
- b. El acceso a las terminales desde los que el usuario se conecta a la red. Ellos pueden incluir desde computadores protegidos a tarjetas inteligentes. Con frecuencia son estos puntos externos de las redes los que necesitan ser protegidos de forma más estricta, mientras que en otros casos se permite el acceso desde cualquier terminal y los controles se centran solamente en el servidor accedido.

En la mayoría de los casos este servicio se implementa íntimamente ligado a la provisión previa de un servicio de autenticación. Una vez que el usuario ha demostrado que es quien dice ser se le aplican restricciones o permisos correspondientes.

En cuanto al grado de implantación de este servicio, cabe decir que, desafortunadamente, con demasiada frecuencia el control se limita a decir sí o no al intento de acceso al recurso, sin mayores detalles posteriores.

También con demasiada frecuencia el control de acceso se aplica a través de mecanismos de autenticación muy débiles, como puede ser una palabra de paso (password) o un PIN (número de identificación personal). En otros casos se emplean mecanismos de criptográficos robustos que aportan la necesaria seguridad en la protección de acceso. Las tarjetas inteligentes representan un componente de seguridad importantísimo de cara a la implantación tanto del servicio de control de acceso como de los restantes servicios de seguridad.

Como ejemplo de aplicación telemática que requiere este tipo de servicios valdría un sistema operativo distribuido. En este tipo de sistemas operativos, se suelen ofrecer facilidades para compartir ficheros, directorios, dispositivos, etc., pero se necesita dar ciertos permisos a determinados usuarios para permitir un uso eficiente y robusto de estos. Si se cumple el servicio de control de acceso se puede decir que se cumplen todos los requisitos de permisos.

1.2.5 Disponibilidad: es la propiedad que tiene un sistema o recurso de un sistema de estar accesible y utilizable a petición de una entidad autorizada, según las especificaciones de rendimiento para el sistema (un sistema está disponible si proporciona servicios de acuerdo con el diseño del sistema en el momento en que los usuarios lo soliciten). Una variedad de ataques puede dar como resultado la pérdida o reducción de la disponibilidad. Estos ataques pueden ser de denegación de servicio.

Anonimato: se trata de conseguir que la identidad de la persona que realiza una determinada operación de comunicación permanezca oculta ante algunos de los actores presentes en esa operación. Se trata de emular en la red situaciones de la vida real en las cuales es conveniente mantener cierto anonimato. Si dentro del correo postal es posible enviar cartas de forma anónima, también el correo electrónico debe permitir esa posibilidad.

Por lo general, para proveer el servicio de anonimato en un escenario de relativa complejidad se necesitan Agentes Telemáticos especializados (TTP) además de las TTPs necesarias para soportar

una infraestructura de seguridad convencional. Será necesario, también, utilizar mecanismos criptográficos avanzados, algo más complejos que los que se refieren en el capítulo dos.

En la Tabla siguiente se muestra una serie de analogías entre los servicios de seguridad y la vida cotidiana.

Servicio de seguridad	Ejemplo de la vida cotidiana
Autenticación	Carné con identificación fotográfica Huellas dactilares
Control de acceso	Llaves y cerrojos
Confidencialidad	Tinta invisible Carta lacrada
Integridad	Tinta indeleble
No repudio	Firma notariada Correo certificado

Tabla Analogías entre servicios de seguridad y vida cotidiana.

La recomendación X.800 define cada uno de estos servicios de seguridad como un servicio proporcionado por una capa de protocolo de sistemas abiertos de comunicación, que garantiza la seguridad adecuada de los sistemas o transferencia de datos. La podemos encontrar en RFC 2828.

En X.800 los divide en cinco categorías y 14 servicios específicos.

1.3 Amenazas, Vulnerabilidades y Ataques en las Redes

1.3.1 ATACANTES

Tipos de Atacantes

Hackers

Un hacker es aquella persona que trabaja con computadores para manipular la tecnología y la información. Es aquella persona que trata entrar en los computadores de diversas maneras sin tener autorización y, por tanto, están realizando un acto ilegal.

Una definición muy buena dada por

Un Hacker es a todas luces, alguien con profundos conocimientos sobre una tecnología. Esta puede ser la informática, electrónica o comunicaciones. El Hacker normalmente conoce todos los terrenos en los que reposa la actual tecnología.

Así pues, el verdadero Hacker es alguien que tiene ansias por saberlo todo, le gusta la investigación y sobre todo lo que resulta más difícil de descifrar. Nos estamos refiriendo a sistemas de cifrado o sistemas de codificación. En la actualidad los sistemas de cifrado y codificación están al orden del día, tomemos como ejemplo los canales de televisión de pago o cualquier soporte de grabación de datos como el CD o DVD.

Los hackers son programadores. Tienen un conocimiento de los lenguajes de programación y de los Sistemas operativos.

Los hackers emplean los mensajes ICMP para examinar las redes o para redireccionar tráfico.

Los hackers intentan conseguir que los usuarios digan sus passwords, esto es lo que ellos llaman Ingeniería Social.

Los hackers realizan programas que automáticamente chequean la seguridad de la red de máquinas remotas para descubrir los puntos más vulnerables y poder entrar en ellas y así romper la seguridad de éstas.

Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en computadores remotos, con el fin de decir aquello de " he estado aquí " pero no modifican ni se llevan nada del computador atacado.

Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones o emplea muchas horas delante del computador, pero para nada debe ser un obsesivo de estas máquinas. No obstante, puede darse el caso.

Este grupo es el más experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

Crackers

El cracker es aquella persona que se dedica a romper los esquemas de protección y de cifrado. El cracker intenta romper la integridad del sistema de seguridad de una máquina remota. No tienen autorizado el acceso y destruyen información muy importante, es decir, se dedican a realizar acciones malvadas.

Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas. Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección.

Pero el problema no radica hay, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado más adelante.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica. Más adelante hablaremos de los Cracks más famosos y difundidos en la red.

A diferencia de los hackers, los crackers no implementan programas para chequear la seguridad de la red, si no que los piden o los roban.

Los crackers pueden romper un sistema para lucrarse, es decir, porque es contratado por una empresa para romper el sistema de seguridad de otra y a cambio recibe un dinero.

Muchas veces oímos hablar de **Cracking**, el cual es el proceso por el cual se intenta descubrir la contraseña de una cuenta de usuario conociendo su contraseña cifrada. Para ello, se cifra cada una de las palabras almacenadas en un diccionario (en este contexto, una serie de palabras formadas por

símbolos empleados en el lenguaje escrito, no sólo por caracteres alfanuméricos) usando el mismo algoritmo que el sistema operativo a atacar. Si el resultado obtenido es igual que la contraseña cifrada, la palabra del diccionario que se cifró es la contraseña buscada.

Lammers

Este grupo es quizás el que más número de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un computador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro computador, le fascinan enormemente.

Este es quizás el grupo que más peligro acontece en la red ya que ponen en práctica todo el Software de Hacking que encuentran en la red. Así es fácil ver como un Lamer prueba a diestro y siniestro un " bombeador de correo electrónico " esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se mofa autodenominándose Hacker.

También emplean de forma habitual programas Sniffers para controlar la Red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada más que cometer el error de que poseen el control completo de tu disco duro, aun cuando el computador está apagado. Toda una negligencia en un terreno tan delicado.

Copyhackers

Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año más de 25.000 millones de pesetas sólo en Europa.

En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los " bucaneros " personajes que serán detallados más adelante.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello " extraen " información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes es el dinero.

Bucaneros

Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que, dentro de ella, los que ofrecen productos " Crackeados " pasan a denominarse " piratas informáticos " así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

Phreaker

Es una extensión del Hacking y el Cracking. Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo, es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesamiento de datos.

Newbie

Es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.

Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

Script Kiddie

Denominados Skid kiddie o Script kiddie, son el último eslabón de los clanes de la Red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack en su estado puro. En realidad, son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red. En realidad, se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los ficheros Readme de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos su propio computador. Esta forma de actuar es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de Hacking. Podrían llamarse los "pulsadores de botones" de la Red. Los Kiddies en realidad no son útiles en el progreso del Hacking.

Ingeniería social

La ingeniería social es quizás la base de un Hacker, para obtener los datos o lo que le interesa por medio de una conversación y de personas. Es la forma de engañar al otro, y hacerle creer que tú eres alguien en quien confiar.

Conjunto de actividades orientadas a establecer alguna relación social (amistad, aprecio, amor, etc.) con personas que pueden facilitar, consciente o inconscientemente, el ataque a un sistema informático.

Una buena muestra de ello es el timo de telefónica, en el que te llaman haciéndose pasar por un técnico de la compañía y te solicitan que teclees un número después de colgar. Este comando llamado ATT, le permite al ingeniero social, realizar llamadas a través de tu teléfono. Se hacen pasar por ser un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente.

Vía el internet o la [web](#) se usa, adicionalmente, el envío de solicitudes de renovar permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas". Llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, -por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco- en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

La principal defensa contra la ingeniería social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas.

Uno de los ingenieros sociales más famosos de los últimos tiempos es [Kevin Mitnick](#). Según su opinión, la ingeniería social se basa en estos cuatro principios:

- * **Todos queremos ayudar.**
- * **El primer movimiento es siempre de confianza hacia el otro.**
- * **No nos gusta decir No.**
- * **A todos nos gusta que nos alaben.**

1.3.2 AMENAZAS Y SUS TIPOS

Las amenazas de un sistema informático se pueden clasificar según diferentes criterios, en los cuales estaremos desarrollando varios de ellos.

Las amenazas o ataques que puede recibir un sistema son muy variados y dependerán en gran medida del origen, éstas pueden ser:

- Internas.
- Externas.

Las **amenazas internas** son aquellas que se originan en las redes de la organización a la que pertenece el sistema atacado; si el sistema no está conectado en red, se dice que el ataque es interno si tiene su origen en la propia consola del sistema. Normalmente, el atacante es algún empleado de la organización propietaria del sistema, pudiendo ocurrir que el ataque no sea premeditado, sino más bien fruto de un despiste o descuido. Si el atacante no mantiene ninguna relación con la empresa, se habrá introducido en ella mediante algún tipo de engaño (ingeniería social).

Las **amenazas externas** se realizan desde sistemas conectados a una red distinta de las de la empresa dueña del sistema objetivo del ataque. También se pueden clasificar las amenazas teniendo en cuenta la motivación del atacante:

a) **Venganza:** El objetivo de algunos hackers es el de dañar los sistemas de una empresa como respuesta a una demanda no satisfecha o un servicio insuficiente. Este grupo está formado principalmente por empleados y clientes de la empresa. Los empleados resentidos, a su vez, se pueden dividir en dos subgrupos: los que siguen en activo dentro de la empresa y los que han sido despedidos.

Normalmente, el grupo de empleados molestos que siguen en activo es el más peligroso, ya que tienen más facilidad para acceder al sistema. Los empleados que ya no trabajan en la empresa intentarán acceder al sistema desde el exterior empleando su vieja cuenta de usuario (desgraciadamente, la mayoría de los administradores de sistemas no anulan las cuentas y privilegios de los usuarios del sistema que causan baja). En determinados casos, buscarán apoyo en antiguos compañeros.

b) **Exaltación del propio ego:** Existen otros hackers cuya finalidad no es otra que la de demostrar que son capaces de acceder a casi cualquier sistema. Generalmente, informan al responsable del sistema atacado de las debilidades encontradas y procuran difundir sus hazañas (no le sirve de nada conseguir atacar un sistema si nadie se entera).

c) **Fines económicos:** Quizás el grupo más numeroso de hackers (y quizás más peligroso por la naturaleza de su motivación y el anonimato de sus acciones) es el formado por aquellos que intentan acceder a los sistemas con fines lucrativos, ya sea para conseguir información privilegiada o confidencial que pueda interesar a una tercera persona, o para provocar graves perjuicios económicos a un directo competidor.

d) **Fines políticos:** Por último, se pueden encontrar también hackers cuya intención es la de conseguir secretos de un partido político o de estado para desestabilizar un gobierno o un partido político. En la actualidad, existen unidades dentro de los diferentes ejércitos destinadas a la guerra electrónica, centradas, entre otras cosas, a lanzar ataques informáticos, y a prevenirlos y evitarlos.

Un ataque son todas aquellas acciones que supongan una violación de la seguridad de nuestro sistema (confidencialidad, integridad o disponibilidad).

Los podemos clasificar de forma genérica según los efectos causados:

- ✚ **Interrupción:** Un recurso del sistema es destruido o se vuelve inestable. Esto es un ataque contra la disponibilidad (Nubes, destrucción Hw, cortar línea de comunicación...).
- ✚ **Intercepción (de datos):** Una entidad no autorizada consigue acceder a un recurso. Esto es un ataque contra la confidencialidad (Obtención de datos con troyanos, copia ilícita de archivos o programas).
- ✚ **Modificación:** Una entidad no autorizada no solo consigue acceder a nuestro recurso si no que es capaz de manipularlo, propio de virus y troyanos. Esto es un ataque contra la integridad (modificación de cualquier archivo de datos, alterar un programa para que funcione de forma distinta...).

- ✚ **Fabricación:** Una entidad no autorizada inserta objetos falsificados en el sistema. Esto es un ataque contra la autenticidad (Inserción mensajes falsos en una red, añadir datos a un archivo). Estos ataques se pueden clasificar en dos tipos:
 - **Activos:** Implican algún tipo de modificación de los datos o la creación de datos falsos (Suplantación de identidad, modificación mensajes, Web Spoofing....).
 - **Pasivos:** No altera la comunicación. Si no que únicamente la escucha o la monitoriza, para obtener de esta manera la información que se está siendo transmitida. Son muy difíciles de detectar pues no alteran los datos. Es posible evitarlos mediante el cifrado de la información y mediante otros mecanismos.

TIPOS DE AMENAZAS

Al conectar el sistema a Internet, se expone a numerosas amenazas que se incrementan diariamente. Los tipos más generales de amenazas son:

- ✚ Vulnerabilidad de información
- ✚ Vulnerabilidad en el software
- ✚ Debilidades en el sistema físico
- ✚ Transmisión de debilidades

Las formas y estilos comúnmente usados en ataques realizados vía Internet en redes corporativas están divididos en 9 categorías:

- ✚ Ataques basados en passwords
- ✚ En base a escuchar el tráfico de la red
- ✚ Ataques que explotan los accesos confiables
- ✚ Basándose en las direcciones IP
- ✚ Introduciendo información sin darse cuenta
- ✚ Predicción de números secuenciales
- ✚ Secuestrando sesiones
- ✚ Ataques enfocados a explotar las debilidades de la tecnología
- ✚ ☐ Explotando el sistema de librerías compartidas

a. Ataques basados en passwords

Estos son, históricamente, uno de los favoritos para los hackers. Inicialmente, los hackers tratan de entrar a un sistema en la red por medio de teclear un nombre de usuario y contraseña. Esta persona tratará de una contraseña a otra hasta que una de ellas funcione. Sin embargo, ahora existen programas que hacen una decodificación o adivinan los passwords mediante una combinación de todas las palabras y letras de diccionarios en varios idiomas con signos de puntuación y números.

b. Escuchando el tráfico de la red

Es posiblemente uno de los más difíciles tipos para llevar a cabo, pero es un ataque muy serio cuando se logra en una transacción comercial. Para ello se utiliza el llamado *packet sniffer*, el cual se encargará de interceptar los paquetes que viajan a través de la red, estos pueden contener información confidencial como las claves de usuarios, paquetes de transacciones comerciales con el número de una tarjeta de crédito, e_mail, etc... El procedimiento es obtener el IP que recibirá el paquete y así cuando pase uno dirigido a ese host, entonces lo copiará para enviarlo al sistema del hacker.

c. Mediante accesos confiables

Son comunes en redes que usan un sistema operativo (incluyendo UNIX, VMS y NT) que incorpora mecanismos de accesos confiables. Los usuarios de estos sistemas pueden crear archivos de hosts confiables (como archivos .rhosts en los directorios base) los cuales incluyen los nombres de máquinas o direcciones IP de las cuales un usuario puede acceder el sistema sin una contraseña para ello. Si un hacker obtiene el nombre de la máquina tendrá privilegios de entrar al sistema y la mayoría de ellos sabe que los administradores de UNIX colocan el archivo en el directorio raíz, con esto se moverían como super-usuarios.

d. Con direcciones IP

Como ya sabemos, cuando las computadoras se comunican en la red, lo hacen mediante el direccionamiento de paquetes. Estas direcciones son las llamadas *IP Address* que identifican cada computadora en el mundo. Cuando un hacker hace un ataque de esta manera, da información falsa acerca de la identidad de su computadora, es decir, dice que su computadora es una confiable dentro de una red mediante el duplicado de una dirección TCP/IP. Así el intruso gana los paquetes de acceso a un sistema y sus servicios.

e. Introduciendo información

Este tipo de ataques se han convertido en comunes y mucho más peligrosos en tanto más usuarios se conectan a la red. Un ejemplo simple es cuando un hacker envía un e_mail a los usuarios informando que el administrador de la red es un intruso y le pide que le envíen su password por este medio y evitar el daño. También se puede hacer usando un applet de Java para avisar que tiene un e_mail nuevo y que necesita poner su clave de acceso para revisarlo, este applet crea una ventana familiar a la vista del usuario para ganar su confianza y es así como se logra obtener su clave. Este tipo de ataque es usual en los usuarios que no conocen mucho acerca de las computadoras y las redes, lo mejor para evitar estos problemas es la educación del usuario.

f. Predicción de números secuenciales

Es una técnica común para el robo de IP's dentro de las redes UNIX. El principio de cualquier conexión TCP/IP requiere que las dos máquinas intercambien lo que se llama un "*handshake*," o un paquete de inicio el cual incluye *números secuenciales*. Las computadoras usan estos números como parte de cada transmisión durante la conexión. La creación de estos se realiza basándose en los relojes internos de cada computadora. En muchas versiones de UNIX, los números secuenciales obedecen un patrón que es predecible usando un determinado algoritmo. Después de escuchar estos patrones durante cierto tiempo, hechos por conexiones legítimas, un hacker puede predecir en cierta medida la secuencia de números para lograr un handshake no autorizado.

g. Secuestro de sesiones

En este tipo, el intruso encuentra una conexión existente entre dos computadoras, generalmente de un servidor y un cliente. Inmediatamente después penetrando a routers desprotegidos o firewalls inadecuados, obtiene los números de direcciones TCP/IP en un intercambio entre las computadoras.

Después el intruso secuestra la sesión del usuario simulando la dirección del usuario. Al lograr esto, el secuestrador se adueña de la sesión y el host desconecta al usuario legítimo y el intruso obtiene libre acceso a los archivos que el usuario podía llegar. Es muy difícil detectar una sesión secuestrada y lo que se puede hacer para evitar esto es, por ejemplo, remover cuentas de acceso innecesarias, conseguir parches de seguridad para proteger los routers y los firewalls, también se puede usar el encriptamiento de paquetes. Es muy importante que se tengan estas medidas porque es virtualmente imposible detectar sesiones secuestradas ya que el secuestrador aparece en el sistema como el usuario secuestrado.

h. Explotando las debilidades de la tecnología

Todos los sistemas operativos tienen sus propias debilidades, algunos son más accesibles que otros. Cuando salen los nuevos sistemas pueden contener los llamados bugs que provocarían el colapso de un equipo conectado a la red.

i. Explotando las librerías compartidas

Esto es muy común en los sistemas UNIX. Una librería compartida es un conjunto de funciones de programas comunes que el sistema operativo carga de un archivo a la memoria RAM en cada petición del programa.

Los hackers hacen un reemplazo de estas librerías para sus propósitos, como proveerlos de privilegios para acceder una petición. La solución a este problema es muy simple, se necesita de un buen mantenimiento del sistema de archivos periódicamente y hacer algunas pruebas.

El estudio de estos problemas es importante ya que ofrecen un amplio panorama de lo que los hacker pueden hacer en cualquier intento de ataque a una red. También podemos revisar las características de cada uno de estos tipos de amenazas para prevenir cualquier intrusión al sistema.

Las políticas de seguridad se deben escribir tomando en cuenta todo lo anterior para establecer una línea de fuego. En caso de ser víctimas de un ataque, es necesario tener algún plan de contingencia respecto a la pérdida de información o el implante de algún programa que le permita el acceso al intruso.

Las características de todos los posibles ataques a una red corporativa o institucional nos permiten la creación de una buena política de seguridad. Esta debe contener la mayor cantidad posible de defensas y/o medidas de prevención. Así mismo, este capítulo nos provee de una visión de lo que debemos revisar en cuanto a posibles trampas, o puertas escondidas dentro de los programas que se van a ejecutar dentro de la red.

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, (como por ejemplo un archivo o una región de memoria principal) a un destino (como por ejemplo otro archivo o un usuario). Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- ✚ **Interrupción:** Se produce cuando un recurso del sistema es destruido o llega a ser inutilizable. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación, borrado de registros, archivos, bases de datos, programas, etc.



Figura 1.1. Ataque por Interrupción

- ✚ **Intercepción:** Una entidad no autorizada consigue acceso a un recurso. Esto es, una participación sin autorización por parte de una persona, computadora o programa en una comunicación. Este es un ataque contra la confidencialidad. Ejemplos de este tipo de ataque son escuchar una línea para tomar los datos que circulan por la red (sniffer, es quizás el más difícil de detectar al no producirse una alteración en el sistema), la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de

paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

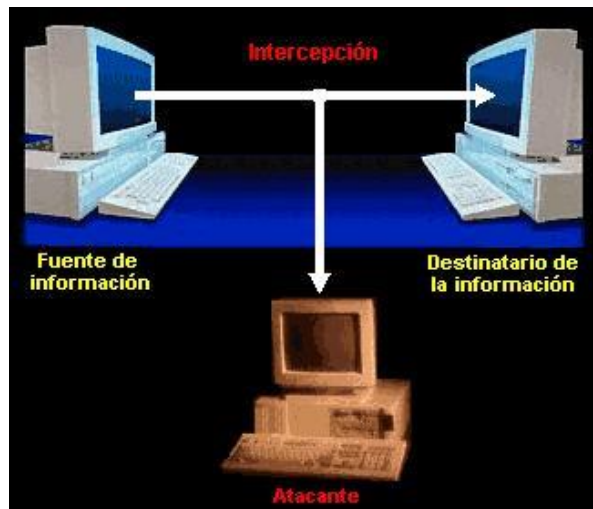


Figura. Ataque por Intercepción

✚ **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo y alterarlo. Este es un ataque contra la integridad. Ejemplos de este tipo de ataque son el cambio de valores en un archivo de datos, alteración de un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red. Este tipo de ataque es el más peligroso.

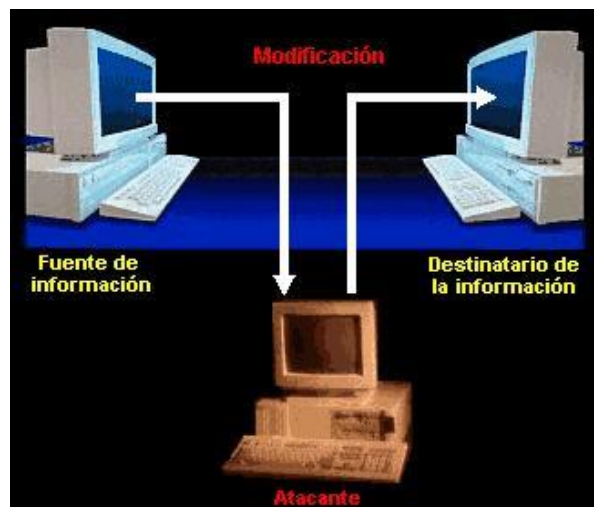


Figura. Ataque por Modificación

✚ **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir registros a un archivo.



Figura. Ataque de fabricación

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Unas de las prácticas actuales para el análisis de intrusos es el hacking ético, ello se utiliza para detectar las posibles vulnerabilidades o falencias en un sistema informático o red de datos. A continuación, se nombrarán algunas herramientas utilizadas para el análisis de redes:

Escáner de red: Escáner de uso general usado para encontrar vulnerabilidades potenciales en la red de la empresa. (También se podría incluir a los escaners de redes VoIP). Estos escaners sirven a su vez para auditar redes LAN o WLAN, facilitando el trabajo de indagar en dichas redes.

Escáner de Puertos: El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuegos.

Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

Escáner para la seguridad de aplicaciones Web: Permite a los negocios realizar evaluaciones de riesgo para identificar las vulnerabilidades en aplicaciones web y así evitar ataques. Este tipo de escaners deberían ser utilizados también por el departamento de desarrollo (programación) de una aplicación web, ayudando así a encontrar todos los bugs que puedan generarse durante la creación de la aplicación, antes de poner la aplicación a un entorno de producción.

Escáner base de datos: Permite encontrar puntos débiles en bases de datos, protegiendo así el activo más importante de una empresa. Es quizás una de las herramientas más importantes ya que si en la base de datos se llega a radicar un error o una amenaza se verá comprometido el buen nombre y la confianza de la organización.

1.3.3 VIRUS

Un **virus** es un programa destructivo que modifica otros programas insertando copias de sí mismo, en un esfuerzo por ocultar su existencia y propagarse a sí mismo en la red. Esta es una forma molesta de

ataque en el sistema por que se comporta como un parásito. Cuando el programa infectado es ejecutado, también se ejecuta el código viral.

Aunque, dependiendo de la naturaleza de los virus, el código original puede o no puede ser ejecutado.

Los virus no pueden ejecutarse como un programa independiente; ellos necesitan un programa anfitrión (host program) que los inicialice. Una vez que el virus se ha establecido y atacado a otros programas en el sistema, es difícil eliminarlo.

Un virus computacional comparte muchos de los atributos de los biológicos convencionales. Consiste de tres subsistemas: mecanismo de infección, activador (trigger) y misión. [

No todos los virus son perjudiciales para un sistema, un virus benéfico, por ejemplo, podría comprimir todos los programas en un sistema para conservar espacio en disco y descomprimirlos cuando son ejecutados, permitiendo al programa, llegar a ser ejecutable otra vez.

Las siguientes recomendaciones ayudan a proteger los sistemas de virus computacionales:

- ✚ Centralizar la responsabilidad de mover cualquier archivo entre sistemas, con el fin de proveer un estricto control e inspección minuciosa.
- ✚ Implantar una política de respaldos con respaldos completos del sistema almacenados por largo tiempo (así que el software más estable del sistema operativo y el software de terceros pueda ser recuperado de medios sin infección como parte de la reconstrucción del sistema).
- ✚ Mantener los archivos temporales fuera de los directorios del sistema operativo y de los que soportan productos de software de terceros. Esto no necesariamente protege al sistema y archivos de terceros de una infección externa, sin embargo, hace más ordenada la recuperación, así como reduce la oportunidad de que el virus sea reintroducido en el sistema.
- ✚ Mantener actualizado con la literatura de UNIX para estar atento de epidemias de virus en la comunidad de UNIX.
- ✚ Establecer máscaras de usuarios (umasks) para que los programas escritos por usuarios no puedan ser invadidos por virus que tengan permisos insuficientes.
- ✚ Proteger directorios de forma tal que estos no sean fácilmente contaminados por virus. Desarrollar políticas para el uso de grupos de usuarios en sistemas UNIX, así que un virus proveniente de group ID público no sea capaz de infectar programas compartidos con otros grupos de usuarios.

Tipos de virus.

Existen muchos tipos de virus. Los primeros que aparecieron contaminaban los discos duros y se propagaban a través de archivos y discos contaminados. Aquellos primeros virus se dividían en:

- ✚ **Virus del sector de arranque** (boot), de la tabla de particiones o de asignación de ficheros. El virus se instala (se almacena) en el sector de arranque, en la tabla de particiones o en la de asignación de ficheros del disco duro, con lo que se ejecuta cada vez que se enciende el computador.
- ✚ **Virus de archivo.** El virus se instala en (se añade a) un archivo ejecutable. En algunos casos, el virus era rápidamente detectado porque el archivo ejecutable dejaba de funcionar correctamente. En otros casos (virus troyanos), el archivo ejecutable seguía funcionando correctamente hasta que se producía el evento que provocaba la activación del virus.
- ✚ **Virus multipartitos.** Son virus que se instalan en cualquier parte del disco (en un archivo, en el sector de arranque, etc.).

Han ido apareciendo nuevos virus (siguen existiendo los virus arriba comentados) que emplean nuevas fórmulas de propagación y dañan los sistemas empleando nuevas técnicas:

- ✚ **Virus de macro.** El virus se instala en un archivo de datos (algunas plantillas para edición de documentos pueden incluir pequeños programas que ayuda a realizar tareas rutinarias de edición). Su velocidad de propagación es mayor porque los usuarios comparten con más frecuencia archivos de datos que ejecutables.
- ✚ **Virus en Internet.** El virus llega al computador a través de Internet (al descargar una página WEB, dentro de archivos adjuntos en un mensaje de correo, etc.) Una vez en el computador, intentará usar la red para llegar a otro computador quedando latente en el primero. También reciben el nombre de gusanos.

Los daños que causan los virus actuales no difieren mucho de los que causaban los primeros, incorporando funcionalidades para iniciar ataques de denegación de servicio (incluso contra sistemas de telefonía móvil) y de recopilación de información del sistema infectado.

1.3.3.1 GUSANOS (WORMS)

Los **worms (gusanos)** son programas autoreplicables y autoinicializables, diseminables por ellos mismos de máquina en máquina a través de arrastrarse por la red. Aprovechan los “security holes” (huecos de seguridad) conocidos. Un worm no altera o daña otros programas, pero podría ser un vehículo para otros programas como los virus.

Un worm no necesariamente verifica la máquina atacada para ver si ya está contaminada. Puede causar un rechazo de los servicios por estar usando todo el espacio en disco. Algunas veces estos programas son diseñados para enviar simplemente de regreso al desarrollador información acerca de los sistemas, la cual puede ser usada más tarde para atacar al sistema directamente, y otras veces ellos pueden hacer daño en su trayecto (posiblemente dejando una bacteria o virus en su camino).

Generalmente estas entidades de red gastan mucho de su tiempo recogiendo y procesando archivos de seguridad y de red, intentando encontrar rutas en la misma hacia otros sistemas e intentando adivinar passwords.

Un worm consiste de tres partes: búsqueda de un nuevo host para infectarlo, copia de sí mismo al nuevo host y provocar que la nueva copia sea ejecutada.

Los síntomas del ataque de un gusano se pueden apreciar en los archivos de log (tales como su.log, el cual indicará los numerosos intentos sin éxito de una entidad no autorizada para convertirse en superusuario), significativo incremento en el tráfico de la red (lo cual se manifiesta como una reducción en la capacidad de procesamiento normal), y procesos anormales corriendo en el sistema (los cuales pueden ser desplegados mediante el comando ps – process status).

1.3.3.2 BACTERIAS

Algunas veces también llamadas conejas, **son programas que existen para recuperarse a si mismas, y generalmente afectan un sistema por tomar ventaja de los recursos computacionales que ellas consumen sólo por existir en el sistema.** Más que pegarse a otros programas, como los virus, las bacterias computacionales simplemente al ser ejecutadas se duplican a si mismas.

La bacteria no altera los datos ni destruye archivos. Su propósito es degradar el servicio del sistema, pues dependiendo de cómo es programada, puede empezar a ocupar todo el espacio en disco o los ciclos de CPU muy rápidamente, llevando al sistema a detenerse. Un programa que es de un solo byte de longitud podría consumir 4 GB. De espacio después de sólo 32 ciclos de reproducción. Los más grandes, programas de medida más real podrían necesitar menos ciclos para sobrecargar el sistema.

1.3.3.3 INSECTOS (BUGS)

Un Bug **es un defecto en un programa que causa que este realice algo inesperado. Estos bugs a menudo son destructivos.** Programas escritos en lenguajes de bajo nivel como C o Lenguaje Ensamblador, son especialmente indefensos para los bugs destructivos porque los errores en el direccionamiento de memoria pueden resultar en sobrescribir datos almacenados en áreas usualmente reservadas para el sistema operativo. Sin pensar que lenguajes como C o Ensamblador sean malos, es muy importante que los programadores tomen en cuenta que programas mal escritos, pueden resultar desastrosos.

1.3.4 TROYANOS.

Primeramente, hay que comenzar comentando en qué consiste un programa de acceso remoto o programa de administración remota. Este tipo de programas, conocidos también como RATs (Remote

Administration Tool), se han desarrollado para el control remoto de un PC o un sistema, valga la redundancia. Es decir, permiten un manejo prácticamente total de un PC, que físicamente no se encuentra al alcance de nuestras manos, por medio de una conexión directa desde otro PC. El programa de acceso remoto debe estar instalado en ambos PCs y su comunicación se produce generalmente vía internet o vía red.

Se denomina **Troyano** (o 'Caballo de Troya', traducción más fiel del inglés Trojan Horse aunque no tan utilizada) a un **virus informático o programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información sin consentimiento de su dueño que permite el control de ese computadora por parte de una persona no autorizada, pudiéndose incluso considerar un tipo de virus, ya que la computadora atacada se “infecta” con él.**

CARACTERISTICAS.

- Se aprovecha frecuentemente de bugs y backdoors de los sistemas informáticos, como el Back Orifice o el BackDoor.
- Sólo una de las dos partes del programa (un troyano se instala en ambos PCs) tiene capacidad de controlar (cliente del troyano) mientras que la otra sirve de conexión con el PC controlado (servidor del troyano).
- El usuario del PC que actúa como servidor (el PC controlado) no tiene conciencia o conocimiento de estar comunicado con aquel otro PC. Ni tan siquiera es consciente de haber instalado el troyano en su PC.
- El servidor del troyano se oculta intentando pasar desapercibido para actuar clandestinamente.

TIPOS DE TROYANOS.

Troyanos del tipo cliente/servidor. Infecta una maquina con el servidor y después accede a ella a través del cliente, con el cual conectabas conociendo la IP de la víctima. Los inconvenientes de este sistema son obvios: existe el problema de conseguir que la víctima active un ejecutable en su máquina, y además, necesitamos conseguir su IP más tarde para poder establecer una conexión. El 95,5% de las maquinas, digamos, normales, no están conectadas 24 horas a Internet (aun con la tarifa Plana: P) y tienen una IP dinámica, por lo que tendríamos que encontrarnos con la víctima en el IRC.

Troyano pasivo consiste en que es la maquina infectada la que conecta a donde el atacante desea, y recoge de allí las instrucciones a seguir. Por ejemplo, cuando la maquina conecta a Internet, esta realiza una conexión a un ftp gratuito donde yo he dejado un script, un batch, o un binario, lo recoge y lo ejecuta. De esta manera tenemos la maquina controlada sin preocuparnos de si está conectado o no, y sin saber su IP.


Los Caballos de Troya son probablemente las amenazas programadas más comunes y fáciles de implantar, son programas que imitan a un programa que el usuario quiere ejecutar, pero son realmente diferentes.

Aparentan ser inofensivos, pero permiten violar la seguridad de un sistema, pues se pueden ver como una herramienta estándar de UNIX, aunque hayan sido programados para realizar ciertos actos destructivos cuando se ejecutan por un usuario del sistema con privilegios apropiados.

Desafortunadamente el usuario no está siempre consciente de que un Caballo de Troya ha sido ejecutado hasta que el daño se ha realizado. Un Caballo de Troya puede ser usado para capturar passwords, cambiar permisos a archivos o crear programas set-UID.

Un ataque de Caballo de Troya engaña al usuario en la ejecución de un programa dañando al sistema por tomar ventaja de los permisos de acceso del usuario. Otro modo común de ataque es a través del uso de shar (compartir) los archivos respaldados en cinta –archive. Estos archivos son grandes shell scripts que al ejecutarse realizan autoextracciones de archivos, los cuales fueron previamente respaldados en cinta como parte del script en sí mismo.

Algunas medidas o hábitos para reducir la oportunidad de que el usuario se convierta en víctima de un Caballo de Troya incluyen lo siguiente:

-  Nunca colocar directorios no estándares (incluyendo .o “ ”) en un PATH. Probablemente colocarlo en último lugar del PATH el ..

- ✚ Nunca ejecutar el `shar` de archivos respaldados en cinta, particularmente de procedencia no familiar. Si se necesita ejecutarlos, llevarlo a cabo sólo en un sistema UNIX que no afecte su daño o pérdida total, sino ejecutarlos después de un llamado al sistema `chroot` que limite el impacto que pueda generarse en el sistema de archivos.

1.3.5 BOMBAS LÓGICAS (LOGIC BOMBS)

Bombas lógicas (time bombs): En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar. La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

Las bombas lógicas son características ocultas construidas en un programa ejecutado cuando se cumplen ciertas condiciones, tales como, un cierto conjunto de claves, o cierta fecha alcanzada, modificando dramáticamente su comportamiento.

Las bombas lógicas ejecutan una función, o un conjunto de funciones, que no fueron características intencionales del programa original, siendo las más comunes la destrucción de aplicaciones o datos. Son frecuentemente colocadas por programadores encargados de mantenimiento de sistemas. El famoso virus Miguel Angel, fue disparado por una bomba lógica.

Existen muchos usos legítimos de bombas lógicas. Los time-out son ampliamente usados por los vendedores de software, permiten administrar las provisiones contractuales o reforzar agendas de pago. La ejecución de una bomba lógica no necesariamente es disparada por el reloj.

Las bombas lógicas son frecuentemente perpetradas no por personas ajenas al sistema quienes han ganado acceso no autorizado (ya que ellos prefieren hacer el daño tan pronto como sea posible), sino por usuarios quienes están autorizados para tener acceso al sistema.

Un caso documentado es la bomba lógica de Michael J. Lauffenburger insertada en un programa llamado Cleanup el 20 de marzo de 1991, la cual está dispuesta para activarse el 24 de mayo a las 6:00 PM., siendo sus funciones eliminar el programa de seguimiento (PTP), borrar la base de datos (SAS.DB) y autodestruirse sin dejar una huella. Un compañero de trabajo la descubrió accidentalmente el 10 de abril. Finalmente, Michael fue arrestado el 31 de abril.

La mejor protección contra los desastres de las bombas lógicas es tener bien definidos procesos de administración y mantenimiento de cuentas de usuario. Tales procedimientos serán enfocados para detectar bombas lógicas antes de que éstas tengan la oportunidad de hacer daños.

- ✚ Proteger todos los editores de archivos de inicialización en el directorio Home, de forma tal que sólo el administrador pueda escribir en ellos. También poner el sticky bit en el directorio Home de forma tal que otros usuarios no tengan permitido borrar archivos que ellos no puedan escribir.
- ✚ Si las terminales tienen la habilidad de repetir cadenas de caracteres enviándolos como si fueran escritos en el teclado, deshabilitar este aspecto (o mejor aún, reemplazar la terminal con una que no tenga esta característica).

Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» («cancer routine»). En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

1.3.6 PUERTAS TRASERAS (BACK DOORS)

Las **back doors** (puertas traseras) son conocidas también como trap doors (trampas), aunque entre ellos existen diferencias importantes que se describen en este capítulo. Estos programas son diseñados para abrir una "puerta trasera" en nuestro sistema de modo tal de permitir al creador del backdoor tener acceso al sistema y hacer lo que desee con él.

El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formar redes de botnets.

Algunas veces son insertados maliciosamente en los sistemas, aunque otros los programadores y desarrolladores los escriben usualmente en aplicaciones que requerirán amplios procedimientos de autenticación.

Los back doors permiten al usuario entrar a los programas rápidamente para propósitos de evaluación, depuración, mantenimiento y monitoreo en el proceso de desarrollo de sistemas. Muchas veces los back doors son olvidados y dejados en el código cuando éste es liberado. Potencialmente destructivos los back doors pueden existir en programas por muchos años antes de ser descubiertos.

Los back doors pueden presentar problemas cuando son descubiertos por hackers sin escrúpulos. Es por eso que se consideran una amenaza real a la seguridad del sistema. Uno de los aspectos más significativos de esta amenaza es que se encuentran disponibles para muchos usuarios. Más que requerir un grado particular de conocimientos técnicos y destreza, para estas amenazas se necesita conocer el back door y puede ser fácilmente pasado de boca en boca o enviado por correo electrónico en bulletin boards. La mejor defensa contra un ataque a través de una puerta trasera es obteniendo el conocimiento de ésta, antes de que llegue a ser ampliamente difundida. Por lo cual, una de las mejores protecciones es la comunicación entre administradores de sistemas.

Las puertas traseras permiten a quien los conocen saltarse los métodos usuales de autenticación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. No es por tanto un método de suplantación, si no de saltarse los controles de autenticación o, como su nombre indica, entrar por la "puerta de atrás".

Son fallos de seguridad que se mantienen, voluntariamente o no, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

1.3.7 TRAMPAS (TRAP DOORS)

Las **trampas** son actualmente consideradas como un caso especial de bomba lógica, aunque se parecen a las puertas traseras, dado que son aspectos no documentados o modos de operación de programas que de otra forma son confiables. Sin embargo, mientras que las back doors son deliberadamente explotadas por usuarios conocedores, las trap doors son disparadas por algún conjunto de condiciones de habilitación causando que estas realicen sus acciones destructivas. Estas condiciones podrían ser la hora del sistema o la identificación del usuario al momento de ejecutar un programa.

1.3.8 HUECOS DE SEGURIDAD (SECURITY HOLES)

Los huecos de seguridad son imperfecciones en el diseño de software, que mal usados, otorgan privilegios a usuarios comunes. La mayoría de los servicios en Internet (FTP, TELNET, SENDMAIL) tienen huecos de seguridad.

Los huecos de seguridad se manifiestan en cuatro formas:

1. **Huecos de Seguridad Físicos.** Donde el problema potencial es causado por permitir acceso físico al equipo a personas no autorizadas, donde estas pueden realizar operaciones que no deberían ser capaces de hacer.
2. **Huecos de Seguridad de Software.** Donde el problema es causado por elementos mal escritos de software privilegiado (daemons, cronjobs) los cuales pueden ser utilizados para realizar cosas que no deberían poder hacer.

3. **Huecos de Seguridad por Uso Incompatible.** Donde, por falta de experiencia o por errores propios, el Administrador del Sistema ensambla una combinación de hardware y software el cual cuando se usa como un sistema está seriamente dañado, desde el punto de vista de la seguridad. Es precisamente esta incompatibilidad de tratar de hacer que dos cosas no conectables pero útiles se integren lo que crea un hueco de seguridad.
4. **Selección de una filosofía de seguridad y su mantenimiento.** Este hueco de seguridad se manifiesta como un problema de percepción y entendimiento. El software perfecto, el hardware protegido y los componentes compatibles no trabajarán adecuadamente a menos que se seleccione una política de seguridad apropiada y las partes del sistema se direccionen para reforzarla. Pues aun teniendo el mejor mecanismo de password en el mundo, es tiempo perdido si los usuarios piensan que su nombre al revés es un buen password.

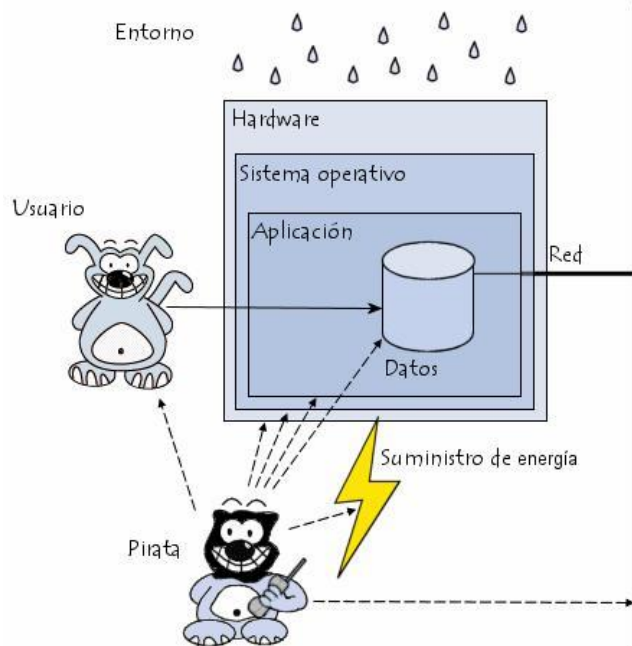
Nuevos huecos como estos son descubiertos y lo mejor que se puede hacer es:

- Tratar de estructurar el sistema de forma tal que el menor número de programas de software posible se ejecute con privilegios de **root/daemon/bin**, los cuales sean conocidos por su robustez.
- Suscribirse a foros donde se obtengan detalles de problemas y soluciones que se apliquen tan rápido como sea posible.

1.3.9 Otros

Los sistemas tanto informáticos como de redes usan una diversidad de componentes, desde electricidad para suministrar alimentación a los equipos hasta el programa de software ejecutado mediante el sistema operativo que usa la red.

Los ataques se pueden producir en cada eslabón de esta cadena, siempre y cuando exista una vulnerabilidad que pueda aprovecharse. El esquema que figura a continuación repasa brevemente los distintos niveles que revisten un riesgo para la seguridad:



HOAX

Un **Hoax** (del inglés: engaño, bulo) es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos informan sobre virus desastrosos, otros apelan a la solidaridad con un niño enfermo o cualquier otra noble causa, otros contienen fórmulas para hacerse millonario o crean cadenas de la suerte como las que existen por correo postal. Los

objetivos que persigue quien inicia un hoax son: alimentar su ego, captar direcciones de correo y saturar la red o los servidores de correo.

Frecuentemente, circulan por Internet falsos mensajes de alerta sobre virus, conocidos como **Hoaxes o bulos**. Su finalidad es generar alarma y confusión entre los usuarios. Para confirmar si ha recibido un falso aviso de este tipo, consulte sitios de confianza como los abajo mencionados.

<http://www.rompecadenas.com.ar/hoaxes.htm>
<http://www.enciclopediavirus.com/tipos/index.php>
<http://www.vsantivirus.com/hoaxes.htm>
<http://esp.sophos.com/virusinfo/hoaxes/>
<http://www.sophos.com/virusinfo/scares/>
<http://www.stiller.com/hoaxa.htm>
<http://www.stiller.com/hoaxes.htm>
<http://hoaxbusters.ciac.org/>
<http://vil.mcafee.com/hoax.asp>
<http://vil.nai.com/vil/hoaxes.asp>
<http://www.trendmicro.com/vinfo/hoaxes/default.asp>
http://www.f-secure.com/hoaxes/hoax_index.shtml
<http://vmyths.com/hoax.cfm?page=0>
<http://hoaxbusters.ciac.org/>
<http://www.urbanlegends.about.com>
<http://www.snopes.com>
<http://www.urbanlegends.com>
<http://securityresponse.symantec.com/avcenter/hoax.html>
<http://www.pandasoftware.es/virus%5Finfo/hoaxes/>
<http://kumite.com/myths/myths/>
<http://antivirus.about.com/compute/antivirus/library/blenhoax.htm>
http://www.f-secure.com/hoaxes/hoax_new.shtml
<http://www.symantec.com/avcenter/hoax.html>

KEYLOGGER

Como su nombre lo indica un **Keylogger** es un programa que registra y graba la pulsación de teclas (y algunos también clicks del mouse). La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas.

Los **Keyloggers físicos** son pequeños dispositivos que se instalan entre nuestra computadora y el teclado. Son difíciles de identificar para un usuario inexperto, pero si se presta atención es posible reconocerlos a simple vista. Tienen distintas capacidades de almacenamiento, son comprados en cualquier casa especializada y generalmente son instalados por empresas que desean controlar a ciertos empleados.

Cabe aclarar que esta forma de actuar puede traer problemas legales a quien lo instala ya que registrar a un usuario mediante este accionar puede interpretarse como una violación a su privacidad. Es aquí donde cobra relevancia una política de seguridad clara, puesta por escrito y firmada por el usuario.

Con respecto a las **keyloggers por software**, actualmente son los más comunes, muy utilizados por el malware orientado a robar datos confidenciales o privados del usuario. Como es de imaginar, la información obtenida es todo lo que el usuario ingrese en su teclado como por ejemplo documentos, nombres de usuarios, contraseñas, números de tarjetas, PINes, etc.

Esto explica el porqué de su gran éxito y utilización actual ya que como sabemos el malware, cada vez más orientado al delito, puede utilizar esta herramienta para proporcionar información sensible del usuario a un atacante.

KeyLoggers físico. http://www.logisteam.org/store/catalog/product_info.php?cPath=21&products_id=29

ROGUE, falsos antivirus gratis

Los **Rogue o Scareware** son sitios web o programas que simulan ser una aplicación de seguridad, generalmente gratuita, pero que en realidad instalan otros programas dañinos. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

Estos programas, que en la mayoría de los casos son falsos antivirus, no suelen realizar exploraciones reales, ni tampoco eliminan los virus del sistema si los tuviera, simplemente informan que se ha realizado con éxito la desinfección del equipo, aunque en realidad no se realizó ninguna acción.

Para los delincuentes es sencillo desarrollar este tipo de software, ya que los programas sólo muestran unas pocas pantallas y unos cuantos mensajes falsos para engañar al usuario.

Por ejemplo, se podría mostrar una pantalla como la siguiente, simulando una exploración del sistema, cuando en realidad son simples imágenes (no dañinas).

Luego de esta supuesta exploración, se podría mostrar un resultado como el siguiente:



Posteriormente, si el usuario es engañado descargaría un programa dañino en su sistema.

ROOTKIT

Un **RootKit** es un programa o conjunto de programas que un intruso usa para esconder su presencia en un sistema y le permite acceder en el futuro para manipular este sistema.

Para completar su objetivo, un Rootkit altera el flujo de ejecución del sistema operativo o manipula un conjunto de datos del sistema para evitar la auditoria.

Un rootkit no es un exploit, es lo que el atacante usa después del exploit inicial. En algunos aspectos, un rootkit es más interesante que un Exploit, incluso que uno 0-day. Algunos de nosotros somos reticentes a creer en el hecho de que más vulnerabilidades continuaran siendo descubiertas. La Seguridad Informática es sobre todo manejo del riesgo.

Un Exploit 0-day es una bala, pero un Rootkit puede decir mucho del atacante, como cuál era su motivación para disparar.

Windows es diseñado con seguridad y estabilidad en mente. El núcleo (kernel) debe ser protegido de las aplicaciones de usuario, pero estas aplicaciones requieren cierta funcionalidad desde el kernel.

Para proveer esto Windows implementa dos modos de ejecución: modo usuario y modo kernel. Windows hoy solo soporta esos dos modos, aunque las CPU Intel y AMD soportan cuatro modos de privilegios o anillos en sus chips para proteger el código y datos del sistema de sobreescrituras maliciosas o inadvertidas por parte de código de menor privilegio.

Originalmente el término **RootKit** proviene de sistemas Unix y hacía referencia a pequeñas utilidades y herramientas que permitían acceso como "root" de esos sistemas.

El término ha evolucionado y actualmente es un conjunto de herramientas utilizadas en cualquier sistema para conseguir acceder ilícitamente al mismo. Generalmente se los utiliza para ocultar procesos y programas que permiten acceso al sistema atacado, incluso tomar control de parte del mismo.

Es importante remarcar que **un Rootkit no es un Malware en sí mismo**, pero, debido a que es utilizado ampliamente para ocultar los mismos, muchas veces se lo considera incorrectamente como programa dañino.

Actualmente, incluso son utilizados por ciertas empresas para controlar componentes del sistema y permitir o denegar su utilización. Hay que remarcar que el uso de estos programas es éticamente incorrecto (o incluso ilegal), ya que se hace sin la autorización expresa del usuario.

SPAM

Se define **SPAM** a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico, pero puede presentarse por programas de mensajería instantánea o por teléfono celular.

El **Spam** es el correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva.

El término spam tiene su origen en el jamón especiado (SPiced hAM), primer producto de carne enlatada que no necesitaba frigorífico para su conservación.

Debido a esto, su uso se generalizó, pasando a formar parte del rancho habitual de los ejércitos de Estados Unidos y Rusia durante la Segunda Guerra Mundial. Posteriormente, en 1969, el grupo de actores Monthy Python protagonizó una popular escena, en la cual los clientes de una cafetería intentaban elegir de un menú en el que todos los platos contenían...jamón especiado, mientras un coro de vikingos canta a voz en grito "spam, spam, spam, rico spam, maravilloso spam". En resumen, el spam aparecía en todas partes, y ahogaba el resto de las conversaciones. Haciendo un poco de historia, el primer caso de spam del que se tiene noticia es una carta enviada en 1978 por la empresa Digital Equipment Corporation.

Esta compañía envió un anuncio sobre su ordenador DEC-20 a todos los usuarios de ArpaNet (precursora de Internet) de la costa occidental de los Estados Unidos. Sin embargo, la palabra spam no se adoptó hasta 1994, cuando en Usenet apareció un anuncio del despacho de los abogados Lawrence Cantera y Martha Siegel. Informaban de su servicio para rellenar formularios de la lotería que da acceso a un permiso para trabajar en Estados Unidos. Este anuncio fue enviado mediante un script a todos los grupos de discusión que existían por aquel entonces. Algunas de las características más comunes que presentan este tipo de mensajes de correo electrónico son:

- La dirección que aparece como remitente del mensaje no resulta conocida para el usuario, y es habitual que esté falseada.
- El mensaje no suele tener dirección Reply.
- Presentan un asunto llamativo.
- El contenido es publicitario: anuncios de sitios web, fórmulas para ganar dinero fácilmente, productos milagro, ofertas inmobiliarias, o simplemente listados de productos en venta en promoción.
- La mayor parte del spam está escrito en inglés y se origina en Estados Unidos o Asia, pero empieza a ser común el spam en español.

Aunque el método de distribución más habitual es el correo electrónico, existen diversas variantes, cada cual con su propio nombre asociado en función de su canal de distribución:

- Spam: enviado a través del correo electrónico.

- Spim: específico para aplicaciones de tipo Mensajería Instantánea (MSN Messenger, Yahoo Messenger, etc).
- Spit: spam sobre telefonía IP. La telefonía IP consiste en la utilización de Internet como medio de transmisión para realizar llamadas telefónicas.
- Spam SMS: spam destinado a enviarse a dispositivos móviles mediante SMS (Short Message Service).

El spam es un fenómeno que va en aumento día a día, y representa un elevado porcentaje del tráfico de correo electrónico total. Además, a medida que surgen nuevas soluciones y tecnologías más efectivas para luchar contra el spam, los spammers (usuarios maliciosos que se dedican profesionalmente a enviar spam) se vuelven a su vez más sofisticados, y modifican sus técnicas con objeto de evitar las contramedidas desplegadas por los usuarios. ¿Cómo funciona? ¿Cómo se distribuye? Obtención de direcciones de correo. Los spammers tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas, es decir, realmente utilizadas por usuarios. Con este objeto, utilizan distintas técnicas, algunas de ellas altamente sofisticadas:

- Listas de correo: el spammer se da de alta en la lista de correo, y anota las direcciones del resto de miembros.
- Compra de bases de datos de usuarios a particulares o empresas: aunque este tipo de actividad es ilegal, en la práctica se realiza, y hay un mercado subyacente.
- Uso de robots (programas automáticos), que recorren Internet en busca de direcciones en páginas web, grupos de noticias, weblogs, etc.
- Técnicas de DHA (Directory Harvest Attack): el spammer genera direcciones de correo electrónico pertenecientes a un dominio específico, y envía mensajes a las mismas. El servidor de correo del dominio responderá con un error a las direcciones que no existan realmente, de modo que el spammer puede averiguar cuáles de las direcciones que ha generado son válidas. Las direcciones pueden componerse mediante un diccionario o mediante fuerza bruta, es decir, probando todas las combinaciones posibles de caracteres.

Por lo tanto, todos los usuarios del correo electrónico corremos el riesgo de ser víctimas de estos intentos de ataques. Cualquier dirección pública en Internet (que haya sido utilizada en foros, grupos de noticias o en algún sitio web) será más susceptible de ser víctima del spam.

Actualmente hay empresas que facturan millones de dólares al año recolectando direcciones de correo electrónico, vendiéndolas y enviándolas mensajes de promociones, ofertas, y publicidad no solicitada.

Las recomendaciones para evitar el SPAM son las siguientes:

1. **No** enviar mensajes en cadena ya que los mismos generalmente son algún tipo de engaño (hoax).
2. Si aun así se deseara enviar mensajes a muchos destinatarios hacerlo **siempre** Con Copia Oculta (CCC), ya que esto evita que un destinatario vea (robe) el mail de los demás destinatarios.
3. No publicar una dirección privada en sitios webs, foros, conversaciones online, etc. ya que sólo facilita la obtención de las mismas a los spammers (personas que envían spam).
4. Si se desea navegar o registrarse en sitios de baja confianza hágalo con cuentas de mails destinada para ese fin. Algunos servicios de webmail disponen de esta funcionalidad: protegemos nuestra dirección de mail mientras podemos publicar otra cuenta y administrar ambas desde el mismo lugar.
5. Para el mismo fin también es recomendable utilizar cuentas de correos temporales y descartables como las mencionadas al pie del presente.
6. **Nunca** responder este tipo de mensajes ya que con esto sólo estamos confirmando nuestra dirección de mail y sólo lograremos recibir más correo basura.
7. Es bueno tener más de una cuenta de correo (al menos 2 o 3): una cuenta laboral que sólo sea utilizada para este fin, una personal y la otra para contacto público o de distribución masiva.

Algunos filtros de correo funcionan efectivamente previniendo gran cantidad de SPAM, pero ninguno funciona lo suficientemente bien como para olvidarnos de estos simples consejos que, utilizados correctamente, nos ayudará a recibir menos correo no deseado. Otra característica negativa de los filtros es que algunos funcionan tan sensiblemente que terminan filtrando correo normal.

ADWARE/SPYWARE

Se define como **Adware** al software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario.

Generalmente, estas aplicaciones agregan iconos gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo. Estas barras de tareas personalizadas tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que el mismo esté buscando.

Se define como **Spyware o Software Espía** a las aplicaciones que recopilan información sobre una persona u organización sin su conocimiento, ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.

Normalmente, este software envía información a sus servidores, en función de los hábitos de navegación del usuario. También, recogen datos acerca de las webs que se visitan y la información que se solicita en esos sitios, así como direcciones IP y URLs que se navegan.

Esta información es explotada para propósitos de mercadotecnia y muchas veces es el origen de otra plaga como el SPAM, ya que pueden encarar publicidad personalizada hacia el usuario afectado. Con estos datos, además, es posible crear perfiles estadísticos de los hábitos de los internautas.

Las recomendaciones para evitar la instalación de este tipo de software son las siguientes:

1. Verifique cuidadosamente los sitios por los que navega, ya que es muy común que estas aplicaciones auto-ofrezcan su instalación o que la misma sea ofrecida por empresas de dudosa reputación.
2. Si es posible, lea atentamente las políticas de privacidad de estas aplicaciones. Generalmente incluyen puntos como "recolectamos la siguiente información del usuario" o "los daños que causa la aplicación no es nuestra responsabilidad" o "al instalar esta aplicación usted. autoriza que entreguemos sus datos a...".
3. Estas aplicaciones normalmente prometen ser barras con funcionalidades extras que se instalan sobre el explorador.
4. Actualmente, se nota una importante aparición de aplicaciones que simulan ser software antispyspyware que en realidad contiene spyware. Una lista de los mismos puede ser encontrada en la dirección que se detalla al pie del presente.
5. Cuando una aplicación intente instalarse sin que usted lo haya solicitado, desconfíe y verifique la lista anterior.
6. Es común que los sitios dedicados al underground o pornográficos, contengan un alto contenido de programas dañinos que, explotando diversas vulnerabilidades del sistema operativo o del explorador, le permiten instalarse.
7. Verificar los privilegios de usuarios. Es común que todos los usuarios que hacen uso de la computadora lo hagan con permisos administrativos. Esto no necesariamente debe ser así, es recomendable que cada usuario tenga su propio perfil, sólo con los permisos necesarios para realizar sus tareas. Ya que esto disminuye el campo de acción de un posible intruso (virus, backdoor, usuario no autorizado, etc.).
8. Estas aplicaciones evolucionan continuamente por lo que contar con un antivirus actualizado y con capacidades proactivas es fundamental para detectar estas aplicaciones y evitar su instalación.

Los programas espías son aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Los datos recogidos son transmitidos a los propios fabricantes o a terceros, bien directamente, bien después de ser almacenados en el ordenador. El spyware puede ser instalado en el sistema a través de numerosas vías, entre las que se encuentran: troyano, que los instalan sin consentimiento del usuario; visitas a páginas web que contienen determinados controles ActiveX o código que explota una determinada vulnerabilidad; aplicaciones con licencia de tipo shareware o freeware descargadas de Internet, etc. El spyware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento de la recogida de datos y la forma en que son posteriormente utilizados.

Antispyware sospechosos: http://www.spywarewarrior.com/rogue_anti-spyware.htm

Este sitio ofrece una lista de software sospechoso. La lista es mantenida por Eric L. Howes profesor en la GSLIS (Graduate School of Library and Information Science) de la Universidad de Illinois, EE.UU.

TIPOS DE ATAQUE SEGÚN SU FORMA DE ACTUAR

a. ESCANEEO ESTADO DE PUERTOS:

Consiste en buscar puertos abiertos y fijarse en los que pueden ser receptivos o de utilidad. Pongamos un símil: Cuando efectuamos una llamada a un número de teléfono podemos saber su estado en ese preciso momento, si está comunicando, averiado, da señal, ...

Así que, selecciona un rango de IPs y hacer esas llamadas de manera consecutiva, aunque debido al firewall se ha cambiado el método escaneando de manera no consecutiva las IPs y los puertos de cada una de ellas. Para entenderlo explicaremos como se realiza la comunicación entre dos PCs. Cuando dos PCs se ponen en comunicación se establece una relación de Cliente, el servidor que escucha todo lo que llega a sus puertos se identifica por medio de su IP y de un puerto determinado. El cliente establece la conexión con el servidor a través de dicho puerto, que debe estar abierto y disponible.

Antes de empezar a cambiar datos se realiza una operación cuya finalidad es reconocerse mutuamente. A esta operación se la conoce como **HandShake** (saludo) y se realiza en el protocolo TCP.

Este saludo se realiza en tres pasos:

- 1-. El cliente 'dice' al servidor que quiere comunicarse con el enviándole un segmento SYN (Synchronize Sequence Number).
- 2-. El servidor (si está abierto y escuchando) al recibir este segmento SYN (activa su indicador SYN) enviar un acuse de recibo al cliente. Si el servidor está cerrado envía un indicador RST.
- 3-. El cliente comprueba la respuesta, mediante paquetes ACK (de reconocimiento), y el estado del servidor (si está disponible o no) y dependiendo de ello comienza el intercambio datos

Una vez finalizada la transferencia se realiza otra operación en tres pasos, pero con paquetes SYN en vez de SYN. Es decir, se produce una llamada, se responde a la llamada, se actúa en consecuencia.

ESCANEEO DE CONEXIÓN TCP CONNECT.

Si el puerto escaneado está abierto y a la escucha devolverá una respuesta de éxito, cualquier otra respuesta conlleva que el puerto no está abierto o que no se puede establecer conexión con este.

No **necesita de privilegios especiales** y se realiza a gran velocidad. Es un **método fácilmente detectable** ya que se verán un montón de conexiones y mensajes de error con una máquina que se conecta y desconecta continuamente.

ESCANEEO TCP REVERSE IDENT.

El protocolo **ident** permite averiguar el nombre de usuario y el dueño de cualquier servicio corriendo dentro de una conexión TCP. Conocido también por **reverse ident**.

FTP BOUNCE ATTACK.

El **protocolo FTP** permite lo que se llama **conexión Proxy FTP**. Es decir, conectarse a un FTP desde un servidor Proxy y al hacer esto establecer una conexión y enviar un archivo a cualquier parte de internet. Esto es aprovechado por los atacantes para realizar escaneos, ya que se realizan detrás de un firewall (el del Proxy), lo que conlleva que sean **difíciles** de rastrear. Son **lentos** y **poco usados**.

ESCANEEO UDP ICMP PORT UNREACHABLE.

Se usa con el protocolo **UDP**, que al ser más simple que el TCP tiene sus desventajas a la hora de escanear ya que al hacer una llamada a un **puerto** este no tiene por qué devolver un respuesta, aunque el servidor del sistema escaneado suele devolver un paquete de error 'ICMP PORT UNREACH' cuando un puerto UDP está cerrado. Técnica muy lenta.

FINGER PRINTING.

Consiste en determinar que SO tiene el computador atacado, Lo normal es ir probando varias técnicas, y según las reacciones del computador víctima, determinar su SO. Hay programas específicos para esta labor. No es una técnica muy efectiva y aunque no es un escaneo en si se usa para llevarlos a cabo.

TCP SYN.

Se envía un paquete SYN, como si se fuera a solicitar una conexión y se espera la respuesta. Al recibir un SYN/ACK se envía inmediatamente un RST (reset) para terminar la conexión y registrar ese puerto como abierto. Pocos sistemas están preparados para detectar este tipo de ataques. En UNIX se necesitan privilegios de administrador para construir estos paquetes SYN

ESCANEO TCP FIN – STEALTH PORT SCANNING.

Escaneo invisible de puertos. Algunos sistemas (FireWalls y **filtros de paquetes**) **monitorizan** la red en busca de paquetes SYN a puertos restringidos. En cambio, los paquetes FYN podrían pasar inadvertidos. Los sistemas Microsoft son inmunes a estos ataques, sin embargo, es posible realizarlo en sistemas Unix.

ESCANEO DE PROTECCION.

En lugar de enviar paquetes completos de sondeo, se parten en un par de pequeños fragmentos IP. Así es más difícil de monitorizar por los filtros que pudieran estar ejecutándose en el sistema atacado. Esta técnica puede producir caídas de rendimiento tanto en el sistema del cliente como en el del servidor, por lo que lo hacen detectable.

EAVESDROPPING-PACKET SNIFFING.

Olfateo de paquetes sin modificarlos. Muchas redes son vulnerables al Eavesdropping o la interceptación pasiva (sin modificación) del tráfico de red. Esto se realiza con paquetes Sniffer (un sniffer es un programa que monitorizan la información que circula por la red) que se centran en las IPs, ya que siempre que se produce una comunicación por la red, en esos paquetes de información se incluyen las IPs de los 2 sistemas que se están comunicando.

SNOOPING-DOWLOADING.

Se parece al sniffing en el sentido de que obtienen información sin modificarla, pero el sistema empleado es distinto ya que con este sistema lo que se hace es copiar la información y bajarla al PC en forma de archivos.

b. ATAQUES DE AUTENTIFICACION.

Consisten, como su nombre indica, en la suplantación de una persona con autorización por parte del atacante. Se suele realizar de dos formas: obteniendo el nombre y contraseña del atacado o suplantando a la víctima una vez ésta ya ha iniciado una sesión en su sistema.

Hay varias técnicas.

SIMULACION DE IDENTIDAD.

Es una técnica para hacerse con el nombre y contraseña de usuarios autorizados de un sistema. El atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta

entrar en él teclea su login y password, el programa los captura y muestra una pantalla de “error en el acceso” al usuario. El usuario vuelve a teclear su login y password, entrando esta vez sin problemas. El usuario cree que en el primer intento se había equivocado al teclear, sin embargo, su login y password han sido capturados por el atacante.

SPOOFING (ENGAÑO).

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Consiste en sustituir la fuente de origen de una serie de datos (por ejemplo, un usuario) adoptando una identidad falsa para engañar a un firewall o filtro de red. Los ataques Spoofing más conocidos son el IP Spoofing, el DNS Spoofing, el Web Spoofing y el fake-mail.

-IP Spoofing.

Sustituir una IP. El atacante logra identificarse con una IP que no es la suya, con lo que, a ojos del atacado, el agresor es una tercera persona, que nada tiene que ver en el asunto, en vez de ser el atacante real.

-DNS Spoofing.

Sustituir a un **servidor DNS** (Domain Name Server) o dominio. Se usan paquetes UDP y afecta a sistemas bajo Windows NT. Se aprovecha de la capacidad de un servidor DNS resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos, ya que éste es su método de trabajo por defecto.

-Web Spoofing.

El atacante crea un sitio Web (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima: datos, contraseñas, números de tarjeta de créditos, etc. El atacante también es capaz de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

Es un ataque peligroso, y difícilmente detectable, que hoy por hoy se puede llevar a cabo en Internet. Afortunadamente hay algunas medidas preventivas que se pueden llevar a cabo:

- 1.- Desactivar la opción de JavaScript en el navegador.
- 2.- Asegurarse en todo momento que la barra de navegación esta activa.
- 3.- Poner atención a las URL que se enseñan en la barra de estado, asegurándote que siempre apuntan al sitio que quieres conectar.

-Fake-mail.

Es otra forma de spoofing y consiste en el envío de e-mails con remitente falso. Aquí el atacante envía e-mails en nombre de otra persona con cualquier motivo y objetivo.

LOOPING.

El intruso usualmente utiliza algún sistema para obtener información e ingresar en otro, que luego utiliza para entrar en otro, y así sucesivamente. Este proceso se llama looping y tiene como finalidad hacer imposible localizar la identificación y la ubicación del atacante, de perderse por la red.

Entre el origen físico y el sistema que finalmente se utilice para realizar una fechoría puede estar plagado de muchos sistemas intermedios, rebasando las fronteras de varios países, dificultando aún más su localización. Otra consecuencia del Looping es que la víctima puede suponer que están siendo atacada por nosotros (si somos el sistema final del looping del atacante), cuando en realidad está siendo atacada por un Insider, o por alguien que se encuentra a miles de kilómetros tanto de nosotros como de la víctima. La localización de la procedencia de un looping es casi imposible de determinar, ya que el investigador debe contar con la colaboración de cada Administrador de cada red utilizada en la ruta del looping, incluso de gobiernos de otros países.

IP SPLICING-HIJACKING

Es un método de sustitución que consiste en que el atacante espera a que la víctima entre en una red usando su nombre, contraseña y demás y una vez que la víctima ha superado los controles de identificación y ha sido autorizada la “tira” del sistema y se hace pasar por ella.

EXPLOITS.

Un **Exploit** es un programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta deficiencia en beneficio del creador del mismo.

Si bien el código que explota la vulnerabilidad no es un código malicioso en sí mismo, generalmente se lo utiliza para otros fines como permitir el acceso a un sistema o como parte de otros malware como gusanos y troyanos.

Es decir que actualmente, los exploits son utilizados como "componente" de otro malware ya que al explotar vulnerabilidades del sistema permite hacer uso de funciones que no estarían permitidas en caso normal.

Existen diversos tipos de exploits dependiendo las vulnerabilidades utilizadas y son publicados cientos de ellos por día para cualquier sistema y programa existente pero sólo una gran minoría son utilizados como parte de otros malware (aquellos que pueden ser explotados en forma relativamente sencilla y que pueden lograr gran repercusión).

ZERO DAY (Día cero): Cuando está aplicado a la información, el "Zero Day" significa generalmente información no disponible públicamente. Esto se utiliza a menudo para describir exploits de vulnerabilidades a la seguridad que no son conocidas por los profesionales del tema.

Se define **Zero Day** como cualquier exploit que no haya sido mitigado por un parche del vendedor.

OBTENCIÓN DE CONTRASEÑAS.

Es la obtención por "Fuerza Bruta" de nombres de usuarios y claves de acceso. Casi todas las contraseñas que utilizamos habitualmente están vinculadas a nuestros nombres reales, nombres de familiares y/o mascotas, fechas significativas, etc. Además, no las solemos cambiar periódicamente. También se suele realizar este tipo de ataques usando una clase de programas llamados **diccionarios**.

DICCIONARIOS.

Los Diccionarios son programas que en su base de datos contienen millones de palabras. Van probando con millones de combinaciones de letras y números encriptados, incluso con caracteres especiales hasta descubrir la combinación correcta de nombre y usuario de la víctima. Son pues programas de fuerza bruta.

c. DENIAL OF SERVICE (DoS). NEGACION DEL SERVICIO.

Ataque de negación de servicio. Se produce la imposibilidad por parte de la víctima de acceder y/o permitir el acceso a un recurso determinado. Por ejemplo, imposibilidad de conectarse, de usar el correo electrónico o, a un mayor nivel, imposibilidad de un servidor de prestar sus servicios. Se basa en el hecho comprobado de que es más fácil corromper un sistema que acceder clandestinamente al mismo. Estos ataques intentan corromper o saturar los recursos de la víctima por medio de peticiones de conexión para lograr desactivarla o impedir el acceso a otros usuarios por medio de la saturación.

JAMMING O FLOODING.

Son ataques que saturan los recursos de un sistema de la víctima dejándola sin memoria, sin espacio libre en su disco duro o saturando sus recursos de red. Los ataques más frecuentes a proveedores son usando el **ping de la muerte** (que bloquea el equipo) o enviando miles de correos electrónicos los usuarios de ese servidor, de forma continuada, saturando los sistemas. Relacionados con el tema están los rabbits (conejos), que son programas que provocan procesos inútiles y se reproducen como conejos hasta que satura la capacidad del sistema, provocando su colapso.

SYN FLOOD.

Ya hemos mencionado que bajo TCP la conexión se realiza en tres pasos. Si en el paso final no llega a realizarse, la conexión permanece en un estado denominado 'semiabierto'. Es el más famoso de los ataques tipo DoS y se basa en un saludo incompleto entre los dos sistemas.

El Cliente envía un paquete SYN pero no responde al paquete ACK del 2º paso del saludo ocasionando que el servidor permanezca a la escucha un determinado tiempo hasta cancelar la llamada. Si se envían muchos saludos incompletos, se consigue que el servidor se paralice o por lo menos se ralentice.

Para operar con este sistema hay que mantener el **Sys Flood** activo, ya que la mayoría de los sistemas tienen un límite de espera muy corto para conexiones semiabiertas. Cuando se ha esperado mucho tiempo, se libera un hueco para aceptar otras posibles peticiones, lo cual puede ser aprovechado para "colar" un paquete SYN destructivo o malicioso. Así que, este ataque se puede utilizar tanto para consumir los recursos de un sistema como para abrir el camino a otro tipo de ataque.

Si este ataque es potente es porque el atacante no necesita apenas potencia en su PC. Con mandar un SYN cada 4 segundos es suficiente. Esta velocidad se consigue de sobra con cualquier modem. Se podría decir que se necesita una velocidad de conexión ridícula. Este ataque suele combinarse también con el IP Spoofing (suplantación de una IP), para ocultar el origen del ataque.

CONNECTION FLOOD.

Se basa en la característica de la mayoría de los proveedores de Internet (ISP) de tener un tope máximo de conexiones simultáneas, que tras ser alcanzado no acepta más conexiones. Si por ejemplo un servidor Web tiene un tope de 1000 conexiones, y el atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita establecer nuevas conexiones para mantener fuera de servicio el servidor.

NET FLOOD.

Se envían tantas solicitudes de conexión que las conexiones de los demás usuarios no pueden llevarse a cabo.

Es un ataque muy dañino y con poca defensa por parte de la red atacada. Es como el típico pesado que no deja de llamarnos por teléfono. Lo único que podemos hacer es descolgarlo, pero entonces no podemos usar el teléfono.

Para solucionarlo el Proveedor tiene que detectar el origen del ataque, bloquear la comunicación desde esa dirección y avisar al administrador de la misma para que actúe, ya que lo normal es que el administrador de esa dirección no sepa nada y que esté siendo utilizada su red para llevar a cabo el ataque por medio de algún spoofing (sustitución). De cualquier manera, saber el origen real del ataque es prácticamente imposible. Una vez se ha solucionado el problema, el servidor puede haber estado colgado durante horas.

LAND ATTACK.

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP en sistemas Windows. El ataque envía a algún puerto abierto de un servidor (generalmente al 113 o al 139) un paquete, maliciosamente construido con la IP y puerto origen igual que la IP y puerto destino. Al final la máquina termina por colapsarse.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto **Smurf o Broadcast Storm**. Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones para a continuación mandar una petición **ICMP** (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. Este paquete maliciosamente manipulado, será repetido en Broadcast, y cientos ó miles de hosts (según la lista de direcciones de Broadcast disponible) mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

SUPERNUKE O WINNUKE.

El **Nuke** es el ataque más común de los equipos Windows, que hace que los equipos que escuchan por el puerto UDP 137 a 139 (utilizados por los protocolos NetBios), queden fuera de servicio o disminuyan su rendimiento al enviarle paquetes o fragmentos UDP manipulados. Generalmente se envían fragmentos de paquetes, que la máquina víctima detecta como erróneos pasando a un estado inestable.

ICMP NUKE.

Éste es un nuke que se basa en el protocolo de control ICMP (Internet Control Message Protocol) que es incorporado al protocolo IP de internet. Este protocolo se encarga de avisar cuando hay un fallo en el sistema de envío de paquetes de un protocolo TCP/IP. Si hay algún fallo (por ejemplo: No route to host), este protocolo se encarga de avisar al TCP/IP, y se corta el envío. ¿Como se usa este nuke? Pues mandando ICMP's falsos, es decir, mandarle al TCP/IP de la víctima un paquete ICMP falseado.

OOB NUKE.

Este ataque, sin el debido parche por parte de la víctima, provoca una caída del sistema bastante violenta. El OOB Nuke (Out Of Band) consiste en mandar cierto paquete de información al puerto 139 de la maquina víctima. Se trata de un bug en los protocolos de comunicación del windows 3.x, 9x y NT, provocando que cuando recibe un paquete con el flag OOB al puerto 139, se produce un fallo de protección general en el sistema. Si enviamos este paquete a dicho puerto, haremos que la maquina objetivo se cuelgue, con la aparición en su pantalla de la pantallita azul con el mensaje: Error de Protección general.

TEARDROP.

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a recomponer correctamente los fragmentos ya que se superponen, haciendo que el sistema se cuelgue. El Windows NT 4.0 es especialmente vulnerable a este ataque. Aunque existen parches que pueden aplicarse para solucionar el problema. Son ataques especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre **Newtear, Bonk y Boink**.

MAIL BOMBING-MAIL SPAMMING-JUNK MAIL.

El Mail Bombing consiste en un envío indiscriminado y masivo de un mensaje idéntico a una misma dirección, saturando así el buzón de correo (mailbox) del destinatario.

El Mail Spaming en cambio es un bombardeo publicitario que consiste en enviar un e-mail a miles de usuarios, haya estos solicitado el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spaming está siendo actualmente tratado por las leyes europeas como una violación de los derechos de privacidad del usuario.

El junk mail o correo basura es una propaganda indiscriminada y masiva a través de e-mails.

El mail spamming y el junk mail no pueden ser considerados como ataques DoS auténticos, porque por mucho que molesten no están encaminados a saturar ningún sistema, aunque en ocasiones se utilicen para que éste se produzca.

ATAQUES DE MODIFICACION – DAÑO.

TAMPERING O DATA DIDDING.

Consiste en una modificación no autorizada de datos o software instalado en el sistema víctima (incluyendo borrado de archivos). Es decir, una vez se ha entrado en un sistema, se modifican o borran

datos del mismo. Ejemplo de este tipo de ataques serían la creación de cuentas falsas, modificación de notas, etc. Suelen realizarse mediante virus o troyanos.

BORRADO DE HUELLAS.

Es una tarea fundamental que realiza un intruso tras haber hurgado en un sistema y terminado su fechoría. Si no lo hace se puede descubrir tanto el origen del ataque como el agujero de seguridad por el que ha entrado el atacante. **Las Huellas** son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en los Logs de los sistemas operativos, de monitores de red y/o sistema, firewalls, ...

COOKIES.

Solo representan una amenaza para la privacidad ya que pueden cumplir la función de espiar. No son capaces de causar daño al sistema. Básicamente se utilizan para reconocer al usuario al entrar en determinados sitios web (foros, por ejemplo) y para contadores de visitas. De todas formas, los navegadores tienen opciones para configurar el ingreso de cookies en nuestro sistema.

ATAQUES USANDO VULNERABILIDADES DE LOS NAVEGADORES.

Son fallos del navegador en sí y no de programas implementados, como pueden ser los controles de JAVA, ActiveX, etc. Los más comunes son los "Buffer Overflow" (desbordamiento de buffer). Debido a una debilidad de los buffers de algunos navegadores para el procesamiento de las entradas de usuario, se puede llegar a manipular datos. Una manipulación común es la de URLs almacenadas.

La realización de estos ataques requiere de un gran conocimiento del lenguaje ensamblador y del sistema operativo del computador atacado. Por ejemplo, se puede modificar una URL para que cuando sea ejecutada por el usuario, se ponga en funcionamiento otra aplicación, como el format, un virus, ... De fallos de este tipo en sistemas Win95 y WinNT se aprovecha, por ejemplo, el virus Nimda.

También se podría realizar este tipo de ataque (Mod-daño) mediante Applets de Java o usando JavaScript o VBScript, de los cuales no se va a hacer mención en este trabajo.

WAREZ

Warez es en realidad software " conocido " que lleva incluido un Crack para ser instalado sin número de serie o en varias máquinas sin pagar por él. En Internet se encuentran infinidad de Warez y números de serie para los programas más conocidos.

Los Warez son una forma de Crackear software y linda con el lado del delito entrando de lleno en él, ya que se violan los derechos de autor.

CARDING

El Carding es una extensión más de esta nueva cibernsiedad y sus constantes búsquedas por controlar todos los sistemas informáticos y electrónicos de la sociedad actual. Hoy por hoy la implantación de las tarjetas de crédito, es masiva y está presente en casi todos los sectores tales como operaciones bancarias, acceso a televisiones de pago, sistemas de pago electrónico y acceso controlado.

El Carding es el estudio de tarjetas chip, magnéticas u ópticas y comprende la lectura de estos y la duplicación de la información vital. Actualmente se ha conseguido clonar las tarjetas GSM, tarjetas de canales de pago y Visa por este procedimiento.

1.3.10 MALWARE, RANSOMWARE, PHISHING Y BOTNET

1.3.10.1 Malware

Este término inglés se refiere al software malicioso que circula por Internet y que constituye un problema cada vez más grave. Con estos programas, que los hackers instalan aprovechando las deficiencias de seguridad de los servidores web, los delincuentes obtienen acceso a sitios web ajenos. Dentro del malware se engloban programas desarrollados con distintos fines, como el adware (que

muestra publicidad emergente no solicitada) y los troyanos (que recopilan información confidencial, como datos bancarios).

Para infectar un equipo a través del navegador web, hay que realizar dos tareas: establecer una conexión con la víctima e instalar el programa en su equipo. En función de la táctica que utilice el hacker, estas dos operaciones pueden suceder muy rápidamente y sin que el usuario se percate de nada.

El beneficio más directo para los creadores de malware se obtiene del robo de información sensible. Tal es el caso de las contraseñas para el acceso a la banca online y otros servicios financieros que hoy en día son posibles a través de Internet: credenciales para el acceso a banca, contraseñas de servicios como PayPal, números de tarjeta de crédito junto con sus códigos secretos... Una vez cuentan con esa información en su poder, realizan transacciones de ciertas cantidades (también a través de Internet o empresas de envío de efectivo) y a través de terceros para obtener directamente los beneficios.

Los datos que interesan a los atacantes. Estos serán sus objetivos predilectos a la hora de recolectar información en un sistema infectado. Estos son: nombres de usuarios y contraseñas, certificados, formularios, correos electrónicos, documentos, tráfico cifrado, datos específicos (espionaje industrial).

Una vez conocidos los datos que pueden llegar a interesar a los atacantes, se describe a continuación los métodos de captura de datos más usados para obtenerlos. Podemos mencionar: registro de teclas pulsadas, análisis del disco duro, phishing local, aplicación que simula al navegador, aplicación superpuesta, formgrabbers, captura de imágenes y videos, rogueware.

Mecanismos frecuentes de distribución de malware:

- **Actualizaciones de software:** El malware envía invitaciones a través de las redes sociales para que los usuarios vean un vídeo y, después, se les hace creer que necesitan una actualización de software para verlo.
- **Publicidad en banners:** Los usuarios hacen clic en un banner que intenta instalar el código malicioso en sus equipos sin que ellos se den cuenta o que le envía a un sitio web donde se les invita a descargar un PDF con código malicioso oculto. También es posible que se les solicite sus datos bancarios para proceder a la descarga.
- **Documentos descargables:** Se anima al usuario a abrir un programa de confianza, como Microsoft Word o Excel, que en realidad contiene un troyano preinstalado.
- **Ataque de interposición "Man-in-the- Middle":** El usuario piensa que se está comunicando con un sitio web de confianza, pero la realidad es que un ciberdelincuente está recopilando la información que ese usuario comparte con el sitio, como su nombre de usuario y contraseña. También es posible que el delincuente se infiltre en una sesión y la mantenga abierta después de que el usuario piense que la ha cerrado, de modo que tiene carta blanca para realizar operaciones fraudulentas. Así, el estafador puede transferir dinero si el usuario había iniciado la sesión en su banco, o bien robar el número de tarjeta de crédito durante una transacción de compra por Internet.
- **Keyloggers:** Se engaña al usuario para que descargue un keylogger con cualquiera de las técnicas descritas anteriormente. Ese programa malicioso hace un seguimiento de actividades específicas, como las acciones del ratón o el teclado, y toma capturas de pantalla para registrar datos bancarios o de la tarjeta de crédito.

1.3.10.2 Ransomware



El ransomware es una de las amenazas informáticas más similares a un ataque sin medios tecnológicos: el secuestro. En su aplicación informatizada, el ransomware es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

El pago generalmente es indicado a través de un depósito bancario, luego del cual el atacante envía las contraseñas para descifrar la información del disco duro. En las primeras versiones, los métodos de cifrado utilizados fueron de lo más precarios y recuperar la información era una tarea viable sin entregar el dinero al atacante. Sin embargo, el ransomware es una amenaza cuyo desarrollo es paralelo a los nuevos métodos de cifrado y su gravedad, por lo tanto, aumenta proporcional al desarrollo de la criptografía.

El ataque, en el común de los casos, ataca solo a ciertos archivos; siendo los principales afectados los de ofimática, como procesadores de texto, hojas de cálculo o diapositivas. También las imágenes y correos electrónicos son considerados prioritarios para el común de los ataques.

El nombre proviene del término sajón "Ransom" que define la exigencia de pago por la restitución de la libertad de alguien o de un objeto, es decir, un secuestro. De todas formas, también se suele denominar a estos ataques como criptovirus.

El nacimiento de este ataque data del año 1989, cuando vía correo postal fueron distribuidos a empresas farmacéuticas, diskettes que supuestamente contenían información respecto al HIV. Al ejecutar los archivos que este contenía, se producían los efectos del ataque: la información del ordenador era cifrada y la víctima podía observar una serie de instrucciones y requerimientos para recuperar sus datos, que incluían la entrega de dinero al atacante.

A pesar que la defensa proactiva de malware es la principal barrera de defensa con la que cuenta el usuario para prevenir esta amenaza; otro método de minimizar los daños por parte del usuario, es la creación de backups periódicos de los datos del ordenador.

1.3.10.3 Phishing

Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc) de forma fraudulenta. El **phishing** es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

El estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

El escenario de Phishing generalmente está asociado con la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. El engaño suele llevarse a cabo a través de correo electrónico y, a menudo estos correos contienen enlaces a un sitio web falso con una apariencia casi idéntica a un sitio legítimo. Una vez en el sitio falso, los usuarios incautos son engañados para que ingresen sus datos confidenciales, lo que le proporciona a los delincuentes un amplio margen para realizar estafas y fraudes con la información obtenida.

La principal manera de llevar adelante el engaño es a través del envío de spam (correo no deseado) e invitando al usuario a acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios. A menudo, estos correos llegan a la bandeja de entrada disfrazada como procedentes de departamentos de recursos humanos o tecnología o de aéreas comerciales relacionadas a transacciones financieras

From: [redacted]
To: [redacted]@yahoo.com.ar
Sent: Monday, December 19, 2011 8:34 PM
Subject: Necesitamos que realices una verificación adicional

SEGU-INFO



Estimado Cliente,

Restringimos algunas funcionalidades de tu cuenta.

¿Por qué?

Esta es una medida preventiva para mantener la seguridad en todas las operaciones de la comunidad de [redacted].

¿Qué tengo que hacer?

1. Ingresar al link que figura al final del mensaje.

1. Llenar el formulario que se le solicitará a continuación con los datos correspondientemente solicitados. Una vez confirmado sus datos su cuenta quedará habilitada para operar.

[https://www.\[redacted\].com/mla/accountSummary](https://www.[redacted].com/mla/accountSummary)



[http://\[redacted\].com/pagos.html](http://[redacted].com/pagos.html)

Otra forma de propagación, menos común, pueden ser el fax y los mensajes SMS a través del teléfono móvil. En algunos casos se proclaman grandes premios y descuentos en la venta de productos. También se debe destacar que el destinatario de los mensajes es genérico y los mensajes son enviados en forma masiva para alcanzar una alta cantidad de usuarios, sabiendo que un porcentaje (aunque sea mínimo) caerá en la trampa e ingresará al sitio falso, donde se le robará la información.

Las recomendaciones para evitar y prevenir este tipo de estafa son las siguientes:

1. Evite el SPAM ya que es el principal medio de distribución de cualquier mensaje que intente engañarlo. Para ello puede recurrir a nuestra sección de Spam.
2. Tome por regla general rechazar adjuntos y analizarlos aun cuando se esté esperando recibirlos.
3. **Nunca** hacer clic en un enlace incluido en un mensaje de correo. Siempre intente ingresar manualmente a cualquier sitio web. Esto se debe tener muy en cuenta cuando es el caso de entidades financieras, o en donde se nos pide información confidencial (como usuario, contraseña, tarjeta, PIN, etc.).
4. Sepa que su entidad, empresa, organización, etc., sea cual sea, **nunca** le solicitará datos confidenciales por ningún medio, ni telefónicamente, ni por fax, ni por correo electrónico, ni a través de ningún otro medio existente. Es muy importante remarcar este punto y en caso de recibir un correo de este tipo, ignórelo y/o elimínelo.
5. Otra forma de saber si realmente se está ingresando al sitio original, es que la dirección web de la página deberá comenzar con **https** y no **http**, como es la costumbre. La **S** final, nos da un alto nivel de confianza que estamos navegando por una página web segura.
6. Es una buena costumbre verificar el certificado digital al que se accede haciendo doble clic sobre el candado de la barra de estado en parte inferior de su explorador (actualmente algunos navegadores también pueden mostrarlo en la barra de navegación superior).

7. No responder solicitudes de información que lleguen por e-mail. Cuando las empresas reales necesitan contactarnos tienen otras formas de hacerlo, de las cuales jamás será parte el correo electrónico debido a sus problemas inherentes de seguridad.
8. Si tiene dudas sobre la legitimidad de un correo, llame por teléfono a la compañía a **un número que conozca de antemano... nunca** llame a los números que vienen en los mensajes recibidos.
9. El correo electrónico es muy fácil de interceptar y de que caiga en manos equivocadas, por lo que jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través de este medio.
10. Resulta recomendable hacerse el hábito de examinar los cargos que se hacen a sus cuentas o tarjetas de crédito para detectar cualquier actividad inusual.
11. Use antivirus y firewall. Estas aplicaciones no se hacen cargo directamente del problema, pero pueden detectar correos con troyanos o conexiones entrantes/salientes no autorizadas o sospechosas.
12. También es importante, que, si usted conoce algún tipo de amenaza como las citadas, las denuncie a algún organismo dedicado a seguridad informática o a la unidad de delitos informáticos de su país.

El **Pharming** es el aprovechamiento de una vulnerabilidad en el software de los servidores DNS que permite a un atacante adquirir el nombre de dominio de un sitio, y redirigir el tráfico de una página Web hacia otra página Web. Los servidores DNS son las máquinas responsables de convertir nombres de Internet en sus verdaderas direcciones IP.

1.3.10.4 Botnet

Botnet o red de ordenadores zombis es el conjunto formado por ordenadores infectados por un tipo de software malicioso, que permite al atacante controlar dicha red de forma remota. Los equipos que integran la red se denominan “zombis”, o también drones.

Formación de un botnet y su funcionamiento:

Aunque los métodos de creación y desarrollo del funcionamiento de una *botnet* son muy variados, se identifican una serie de **etapas comunes** en la vida útil de este tipo de redes:

1. El creador de la *botnet* diseña la red que va a crear, definiendo los objetivos y los medios necesarios que va a emplear, incluido el sistema de control de la red.
2. Además, necesitará un malware que se aloje en los equipos y permita el control del mismo, denominado *bot*, que frecuentemente es un troyano. Este malware puede ser creado por él mismo (el creador de la red) o puede comprar este *bot* a un creador de malware.
3. El siguiente paso consiste en distribuir el malware o *bot* por cualquier método: correo basura, páginas con vulnerabilidades, ingeniería social, etc. El objetivo final es que las víctimas ejecuten el programa y se infecten. En la mayoría de las ocasiones el propio troyano se propaga por sí mismo, y es capaz (como los gusanos tradicionales, pero diseñados específicamente para formar parte de una red concreta una vez infectados) de llegar a otros sistemas desde un sistema infectado a su vez. Si tiene éxito, el número de zombis puede llegar a crecer exponencialmente.
4. Una vez que el atacante consigue una masa crítica suficiente de sistemas infectados, puede conseguir el propósito buscado al programar el sistema. Algunas de estas actuaciones pueden ser:
 - Robar información de los equipos infectados.
 - Enviar correo basura o spam.
 - Realizar ataques combinados a una página web o ataques de denegación de servicio distribuido.
 - Construir servidores web para alojar material ilícito (pornográfico y/o pedofílico), realizar ataques de fraude online (*phishing*), alojar software malicioso.

- Distribuir o instalar nuevo malware.
- Crear nuevas redes de equipos zombis.
- Manipular juegos online.
- Observar lo que la víctima hace si el programa ofrece la posibilidad de visionado de escritorio remoto.
- El creador de la *botnet* puede explotarla de diversas formas:
- Utilizar la red directamente en su beneficio.
- Alquilarla a terceros, de tal forma que el cliente recibe los servicios y el creador controla la red.
- Vender entornos de control, es decir, el creador vende el programa de control de zombis al cliente, para que este último lo explote.

6. La *botnet* permanecerá activa mientras se produzca la actualización del *bot* para dificultar su detección, añadir alguna funcionalidad o alguna otra mejora. El declive de la misma puede provocarse con la resolución de vulnerabilidades de sistemas operativos y aplicaciones tras la publicación por parte de los fabricantes de las actualizaciones, la mejora en el control de las redes, utilización de antivirus y antiespías, etc.

Métodos de control de los botnets

El método de control o protocolo de comunicación de la *botnet* es su núcleo y ofrece diferentes posibilidades al atacante, desde el control de forma segmentada (canales de IRC) al control por medio de sistemas de nombre de dominio (DNS) o control a través de la navegación web (HTTP), entre otros. La evolución de estos protocolos implica a su vez fórmulas más sofisticadas de protección del malware para evitar que la red zombi sea descubierta. La dificultad de realizar esta detección plantea problemas no solo técnicos, sino también judiciales, ya que estas redes suelen propagarse por varios países a la vez, afectando por tanto a varias legislaciones.

Se dan algunos los tipos de protocolos de control de las *botnets*. Estos son:

Puertos fijos y puertas traseras: Los *bot* tradicionales abrían una puerta trasera en un ordenador (un puerto lógico o *socket*) que permitía al atacante conectarse directamente y controlar el sistema infectado. Aunque los programas ofrecían ventajas para gestionar a un gran número de sistemas con la puerta trasera “disponible”, esto resultaba incómodo para el atacante, y no era una forma eficiente de controlar una *botnet*.

IRC (chat): La forma tradicional de control que se ha venido empleando ha sido a través de un típico chat (protocolo IRC o *Internet Relay Chat*). Los sistemas zombis infectados pasan a formar parte de una sala privada, como las tradicionales salas de chat en las que los participantes pueden enviarse mensajes cruzados.

HTTP (web): Para eludir los cortafuegos, los atacantes idearon una nueva forma de comunicar los zombis con el controlador. Prácticamente todos los cortafuegos permitían (y permiten) conexión hacia una web, por tanto, hicieron que los troyanos (*bots*) se comunicaran por este protocolo con el sistema central. Hoy es uno de los métodos más usados, debido a lo complejo que es para el usuario detectar tráfico HTTP (navegación) “anómalo” en su tráfico HTTP habitual. Además, HTTP permite cifrar de forma sencilla el tráfico, lo que hace que los atacantes puedan pasar desapercibidos en mayor medida.

Finalidad de un botnet:

Como se indicaba en el apartado II.3, el creador de una *botnet* necesita reunir un número suficiente de equipos infectados para poder explotarla de la forma más rentable, desde utilizarla directamente a alquilarla o venderla.

Por tanto, los ciberataques que realiza el controlador pueden revestir diversas fórmulas, ilegítimas pero muy lucrativas en su mayoría. Se desarrollan las principales, tales como Fraudes de tipo “click” (publicitario), Denegación de servicio distribuida (DDoS), Robo de información, correo basura, aplicaciones pirateadas, alquiler de botnets

1.4 Vulnerabilidades más comunes que pueden comprometer la seguridad

The SANS Institute (System Administration, Networking, and Security Institute) y el FBI, han venido publicando una extensa lista con las veinte vulnerabilidades más explotadas en la mayoría de los ataques a sistemas computacionales vía Internet.

Recientemente, se ha publicado una actualización de su versión original (en inglés). El listado completo, incluye soluciones y sugerencias de cada vulnerabilidad.

Estos 20 artículos incluyen conocidas vulnerabilidades tanto en Windows, como en Unix, las que son explotadas a menudo por atacantes y programas malévolos, como virus y troyanos.

Sin embargo, es bien sabido que la seguridad puede ser comprometida por muchos motivos, los más comunes se mencionan a continuación:

- **Empleados:** las estadísticas internacionales indican que más del 70% de las violaciones de seguridad en las empresas ocurren internamente, bien sea por personal con ánimos de revancha, o simplemente por mera curiosidad.
- **Sistemas mal configurados:** es práctica muy común instalar los sistemas tal y como los provee el fabricante, sin eliminar servicios ni cerrar puertos que jamás serán utilizados. Por lo general, estas configuraciones por defecto poseen vulnerabilidades que pueden ser explotadas por individuos malintencionados con la finalidad de ingresar a los sistemas
- **Falta de Políticas y Procedimientos que refuercen la seguridad:** un elemento primordial de toda arquitectura de seguridad es el correspondiente a las políticas y generalmente se utilizan tecnologías para reforzar su cumplimiento. La carencia de buenas políticas de seguridad podría permitir que se instalen tecnologías inadecuadas, o incorrectamente, abriendo así brechas en la seguridad de datos corporativa.
- **Herramientas equivocadas:** el uso de herramientas de seguridad es necesario, pero si no se tiene en cuenta el por qué y para que se necesitan, realmente no sirven de mucho; por ejemplo, es posible que se adquieran sistemas de análisis de vulnerabilidades que no sean utilizados ni actualizados regularmente los cuales dejen vulnerabilidades sin detectar en los diferentes sistemas.
- **Inexistencia de Monitoreo:** el uso de herramientas de monitoreo es necesario para la detección oportuna de posibles ataques; más aún, es necesario centralizar las alertas en un único lugar, a fin de poder dar respuesta efectiva y eficiente ante posibles ataques. Sin embargo, cuando se adquiere tecnología puntual de seguridad muchas veces no se toma en cuenta que la información generada por ellas puede ser monitoreada y, en muchas ocasiones, ni siquiera se activan las de auditorías de seguridad de dichos dispositivos permitiendo que los atacantes pasen desapercibidos.
- **Código mal escrito:** cuando se escriben programas, pocas veces se tienen en cuenta las características mínimas de seguridad como, por ejemplo, el evitar que se sobrecarguen variables o que se pasen parámetros no esperados. Esto puede ser aprovechado por los hackers para generar fallas que les permita ingresar a los sistemas.

Referencias Bibliográficas

Delitos Informáticos. Código Penal España. Consultado en Julio, 2015 de URL:
http://libros-revistas-derecho.vlex.es/vid/delitos-introducidos-derecho-comparado-417360006?_ga=1.107115210.993565054.1438801255

Hackers los Piratas del Chip y de Internet. Claudio Hernández. 2001.

Importancia de la seguridad en materia de la informática
<http://csrc.nist.gov/publications/history/ande80.pdf>

Wikipedia:Timeline of computer security hacker history
http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

Seguridad de la información. <http://www.segu-info.com.ar/>

Tarea

1. Un empleado poco satisfecho ha robado varios discos duros de muy alta calidad con datos de la empresa. ¿Qué importa más, el costo de esos discos o el valor de los datos? Justifique su respuesta.
2. En una empresa se comienza a planificar estrategias de acceso a las dependencias, políticas de backup, de protección de los equipos ante fuego, agua, etc. ¿Eso es seguridad física o lógica? ¿Por qué?
3. En nuestra empresa alguien usa software pirata. ¿Es una amenaza de interrupción, interceptación, modificación o de generación?
4. Como supervisores de seguridad hemos detectado que alguien está realizando acciones no lícitas, por ejemplo, copias no autorizadas de información. ¿Qué actitud debemos tomar?
5. ¿Qué medidas serían la más adecuadas de cara a minimizar el ataque por virus en nuestra empresa?
6. Si deseamos que nuestra empresa esté debidamente protegida tanto física como lógicamente, ¿qué debemos hacer?
7. ¿Qué diferencia hay entre el concepto de información y su calidad según lo entienda una empresa o los estudios de ingeniería?
8. ¿Por qué se dice que la información de una empresa es su activo más valioso? Compare este activo con el personal de la misma y póngase en situaciones en las que ambos se pierden, ¿qué situación podría ser es más perjudicial para la continuidad de dicha empresa?
9. Como supervisores de seguridad hemos detectado que alguien está realizando acciones no lícitas, por ejemplo, copias no autorizadas de información. ¿Qué actitud debemos tomar?