Implementación de mecanismos de seguridad activa

Seguridad y Alta Disponibilidad

Autor: Miguel Ángel García Felipe

I.E.S GREGORIO PRIETO

- **ÍNDICE:**

* Sistemas de Detección de Intrusos (IDS).

* Técnicas de Detección de Intrusos.

* Tipos de IDS: (Host IDS, Net IDS).

* Software libre y comercial.

12. Sistemas de seguridad en WLAN.

- Sistema Abierto.

- WEP.

- WPA.

13. Recomendaciones de seguridad en WLAN.

- **Clasificación de los ataques en sistemas personales:**

Digamos que 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, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.
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 fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero 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:

1. **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. 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 o deshabilitar el sistema de gestión de ficheros.

2. **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros 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).

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

4. **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 espurios en una red o añadir registros a un archivo. Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

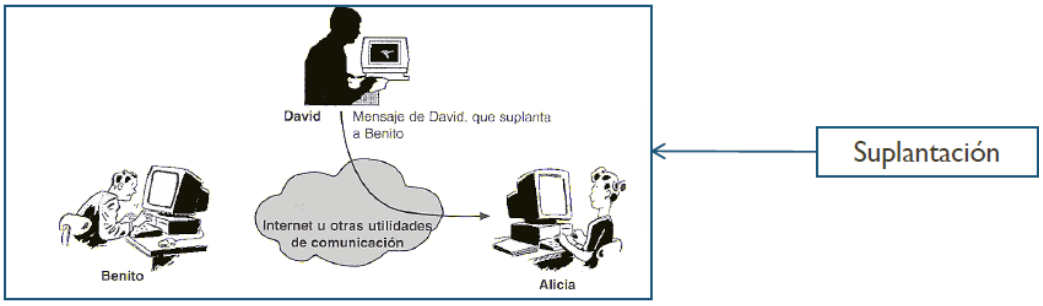
Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
Control de las horas habituales de intercambio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

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

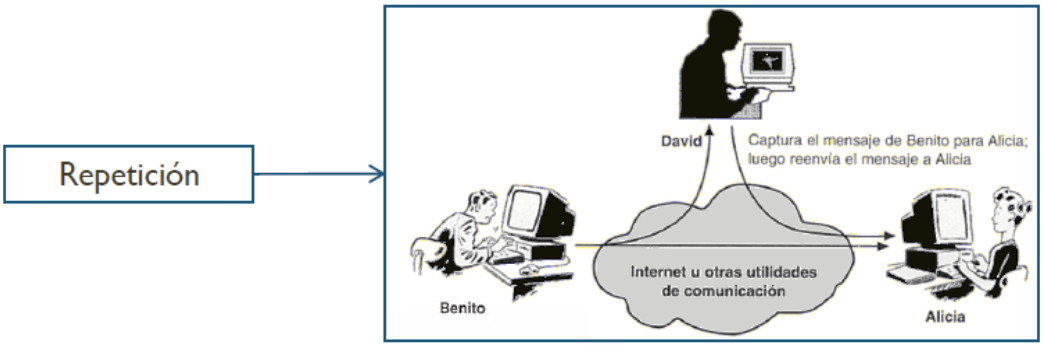
Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

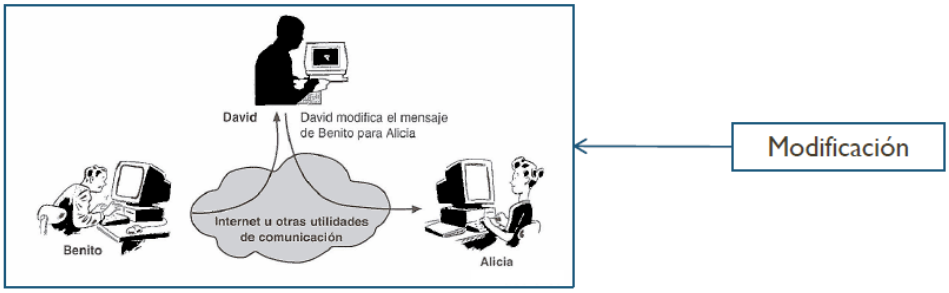
a. **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.



b. **Repetición:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

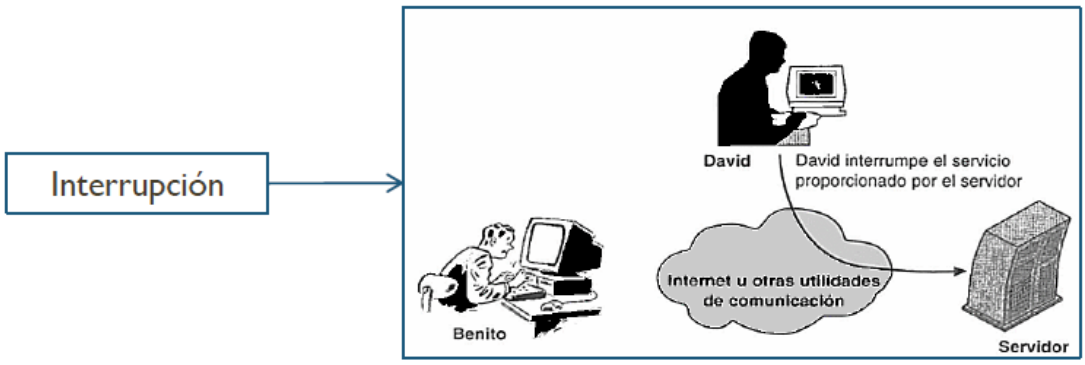


c. **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".



d. **Interrupción:** o degradación fraudulenta del servicio, impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los

mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

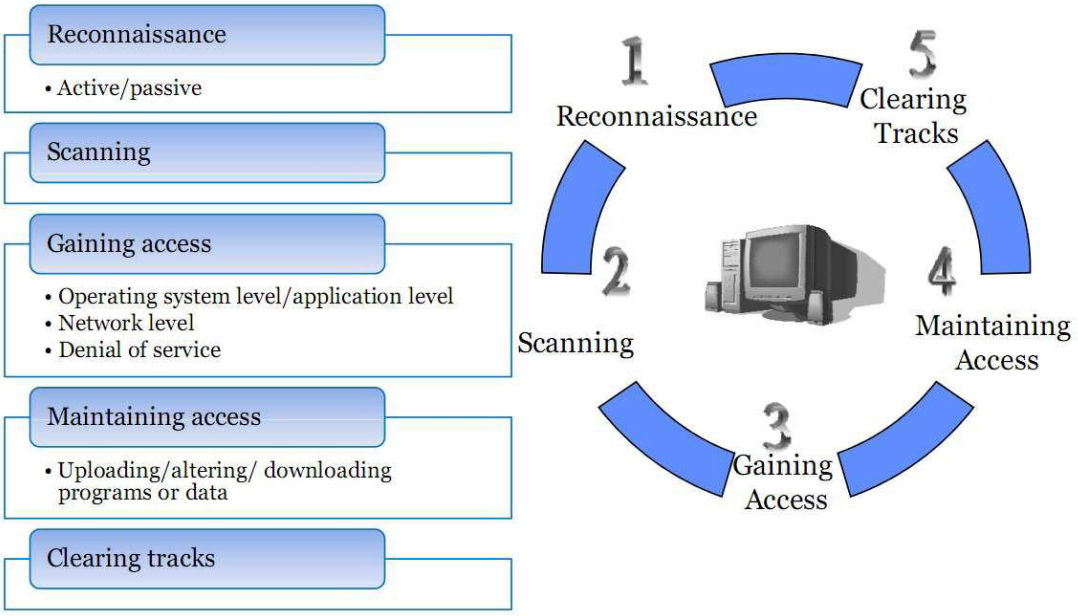


- ## Anatomía de ataques:

Anatomía de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

La siguiente imagen muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado:



Fases comunes de un ataque informático

Básicamente se compone de cinco etapas bien diferenciadas que permiten acceder a un sistema de forma metódica y sistemática.

- **Fase 1: Reconnaissance (Reconocimiento)**. Esta etapa involucra la obtención de información (*Information Gathering*) con respecto a una potencial víctima que puede ser una persona u organización, utilizando diferentes recursos.

  Generalmente se recurre a diferentes recursos de Internet como búsquedas avanzadas a través de Google y otros buscadores para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son: diferentes estrategias de **Ingeniería social** como el **Dumpster diving** (buscar información del objetivo en la basura), el **sniffing** (interceptar información).

- **Fase 2: Scanning (Exploración)**. En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.
  Entre las herramientas que un atacante puede emplear durante esta fase se encuentran:

  - Network mappers
  - Port mappers
  - Network scanners

- Port scanners
- Vulnerability scanners

- **Fase 3: Gaining Access (Obtener acceso)**. En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (*Flaw exploitation*) descubiertos durante las fases de reconocimiento y exploración.
  Algunas de las técnicas que el atacante puede utilizar son:
  - *Buffer Overflow*
  - *Denial of Service (DoS)*
  - *Distributed Denial of Service (DDos)*
  - *Password filtering*
  - *Session hijacking*

- **Fase 4: Maintaining Access (Mantener el acceso)**. Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet.
  Para ello, suelen recurrir a recursos como:
  - Backdoors
  - Rootkits
  - Troyanos

- **Fase 5: Covering Tracks (Borrar huellas)**. Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

- **Análisis del software malicioso o malware:**

Malware (del inglés **mal**icious soft**ware**, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware.

Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos. Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware. Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red.

Siguiendo algunos sencillos consejos se puede aumentar considerablemente la seguridad de una computadora, algunos son:

Protección a través del número de cliente y la del generador de claves dinámicas

- Tener el sistema operativo y el navegador web actualizados.
- Tener instalado un antivirus y un firewall y configurarlos para que se actualicen automáticamente de forma regular ya que cada día aparecen nuevas amenazas.
- Utilizar una cuenta de usuario con privilegios limitados, la cuenta de administrador solo debe utilizarse cuándo sea necesario cambiar la configuración o instalar un nuevo software.
- Tener precaución al ejecutar software procedente de Internet o de medios extraíbles como CD o memorias USB. Es importante asegurarse de que proceden de algún sitio de confianza.
- Evitar descargar software de redes P2P, ya que realmente no se sabe su contenido ni su procedencia.
- Desactivar la interpretación de Visual Basic Script y permitir JavaScript, ActiveX y cookies sólo en páginas web de confianza.
- Utilizar contraseñas de alta seguridad para evitar ataques de diccionario.

Historia: el Malware

Fue en 1949 cuando Von Neumann estableció la idea de programa almacenado y expuso La Teoría y Organización de Autómatas Complejos, donde presentaba por primera vez la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura. Si bien el concepto tiene miles de aplicaciones en la ciencia, es fácil apreciar una aplicación negativa de la teoría expuesta por Von Neumann: los virus informáticos, programas que se reproducen a sí mismos el mayor número de veces posible y aumentan su población de forma exponencial.

En 1959, en los laboratorios de Bell Computer, tres jóvenes programadores: Robert Thomas Morris, Douglas Mcllroy y Victor Vysottsky crean un juego denominado CoreWar basado en la teoría de Von Neumann y en el que el objetivo es que programas combatan entre sí tratando de ocupar toda la memoria de la máquina eliminando así a los oponentes. Este juego es considerado el precursor de los virus informáticos.

Fue en 1972 cuando Robert Thomas Morris creó el que es considerado como el primer virus propiamente dicho: el Creeper era capaz de infectar máquinas IBM 360 de la red ARPANET (la precedente de Internet) y emitía un mensaje en pantalla que decía "Soy una enredadera (creeper), atrápame si puedes". Para eliminarlo, se creó otro virus llamado Reaper (segadora) que estaba programado para buscarlo y eliminarlo. Este es el origen de los actuales antivirus.

En la década de los 80 los PC ganaban popularidad y cada vez más gente entendía la informática y experimentaba con sus propios programas. Esto dio lugar a los primeros desarrolladores de programas dañinos y en 1981, Richard Skrenta escribe el primer virus de amplia reproducción: Elk Cloner, que contaba el número de veces que arrancaba el equipo y al llegar a 50 mostraba un poema.

En 1984, Frederick B. Cohen acuña por primera vez el término virus informático en uno de sus estudios definiéndolo como "Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo".

En 1987 hace su aparición el virus Jerusalem o Viernes 13, que era capaz de infectar archivos .EXE y .COM. Su primera aparición fue reportada desde la Universidad Hebrea de Jerusalem y ha llegado a ser uno de los virus más famosos de la historia.

En 1999 surge el gusano Happy desarrollado por el francés Spanska que crea una nueva corriente en cuanto al desarrollo de malware que persiste hasta el día de hoy: el envío de gusanos por correo electrónico. Este gusano estaba encaminado y programado para propagarse a través del correo electrónico.

En el año 2000 hubo una infección que tuvo muchísima repercusión mediática debido a los daños ocasionados por la infección tan masiva que produjo. Fuel el gusano I Love You o LoveLetter, que, basándose en técnicas de ingeniería social infectaba a los usuarios a través del correo electrónico. Comenzaba aquí la época de grandes epidemias masivas que tuvieron su punto álgido en el 2004.

Fue en ese año cuando aparecieron gusanos como el Mydoom, el Netsky, el Sasser, o el Bagle, que alarmaron a toda la sociedad y lo que buscaban era tener la mayor repercusión y reconocimiento posible. Ese fue el año más duro de este tipo epidemias y curiosamente el último. Los creadores de malware se dieron cuenta de que sus conocimientos servirían para algo más que para tener repercusión mediática… para ganar dinero.

Clasificación de malware

Fue en 2005 cuando, tras 5 años de tendencia sostenida en la que los virus tal y como los conocíamos fueron dejando su lugar a gusanos y troyanos encargados de formar redes de bots para obtener dinero, cuando vieron que el entretenimiento que podía suponer la creación de malware se podía convertir en un negocio muy rentable.
Quizá la mejor prueba de ello sean los denominados Troyanos Bancarios de los que existen miles de variantes dado que los creadores, para dificultar su detección modificaban permanente el código de los mismos.
Este tipo de malware actualmente se distribuye mediante exploits, spam o a través de otro malware que descarga el troyano bancario. Este último tipo de troyano es el encargado de robar información relacionada con las transacciones comerciales y/o datos bancarios del usuario infectado.
Otra amenaza latente relacionada con la obtención de beneficios económicos a través del malware es el spyware y adware, donde algunas empresas de software permiten al usuario utilizar sus aplicaciones a cambio de que los creadores puedan realizar un monitoreo de las actividades del usuario sin su consentimiento.

En cuanto a las amenazas para móviles, no cabe duda de que la llegada de las tecnologías, móviles e inalámbricas, y su constante evolución han revolucionado en los últimos años la forma en la que nos

comunicamos y trabajamos. Sin embargo, la expansión del uso de esta tecnología ha hecho que también se convierta en un vector de ataque importante para la industria del malware. Fue durante el año 2004 cuando se informó de la existencia del primer código malicioso para plataformas móviles: Cabir.A siendo, junto al ComWar.A, los más conocidos, este último no solo por su capacidad de replicarse a través de Bluetooth sino también a través de mensajes de texto con imágenes y sonido (MMS), enviándose a las direcciones y números de la agenda de sus víctimas. Actualmente existe malware para las plataformas más comunes, como pueden ser Symbian, PocketPC, Palm, etc, siendo el método de propagación tan diverso como las posibilidades que nos ofrecen estos avances tecnológicos: SMS, MMS, IrDA, Bluetooth, etc.

A día de hoy la plataforma más atacada es Windows sobre procesadores de 32 bits. Como hemos mencionado anteriormente, los creadores de malware han visto en esta actividad un método de enriquecimiento y pensando en términos económicos y estableciendo el target más amplio posible, los usuarios de plataforma Windows representan el 90% del mercado. Quizás otro obstáculo con el que chocan los creadores de malware para Linux y Macintosh tiene que ver con la capacitación media/alta de los usuarios de este tipo de plataformas, por lo que la Ingeniería Social, principal método de propagación en la actualidad, no resulta tan eficiente con estos usuarios.
Virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Algunas acciones que puede realizar un virus son:

- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.
- Molestar al usuario cerrando ventanas, moviendo el ratón.

Gusano (también llamados IWorm por su apocope en inglés, *I* de Internet, *Worm* de gusano) es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan. Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse. Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (es decir, a otras terminales en la red) y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en diversos métodos, como SMTP, IRC, P2P entre otros.

Troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.

Evitar la infección de un troyano es difícil, algunas de las formas más comunes de infectarse son:

- Descarga de programas de redes p2p y sitios web que no son de confianza.
- Páginas web que contienen contenido ejecutable (por ejemplo controles ActiveX o aplicaciones Java).
- Exploits para aplicaciones no actualizadas (navegadores, reproductores multimedia, clientes de mensajería instantánea).
- Ingeniería social (por ejemplo un cracker manda directamente el troyano a la víctima a través de la mensajería instantánea).
- Archivos adjuntos en correos electrónicos y archivos enviados por mensajería instantánea.

Stealer (en español "ladrón de información") es el nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, tal como su nombre de acceso a sitios web, contraseña o número de tarjeta de crédito.

Infostealer puede afectar también al servicio de correo electrónico MSN Messenger, enviando mensajes falsos e incluso introduciendo en ellos datos incluidos por los usuarios en sus mensajes a través de dicho servicio.

Otro problema causado por stealer puede ser la desconexión involuntaria de un sitio web.

Estos programas pueden detectarse y eliminarse mediante software antivirus, aunque la mejor forma de evitarlos consiste en no abrir documentos anexos a correos electrónicos enviados por remitentes desconocidos o dudosos.

Crimeware es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. El término fue creado por Peter Cassidy, Secretario General del Anti-Phishing Working Group para diferenciarlo de otros tipos de software malicioso.

El *crimeware* (que debe ser diferenciado del spyware, adware) ha sido diseñado, mediante técnicas de ingeniería social u otras técnicas genéricas de fraude en línea, con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas en línea de compañías de servicios financieros (típicamente clínicas) o compañías de venta por correo, con el objetivo de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el *crimeware*.

El *crimeware* puede, de forma subrepticia, instalar un *keylogger* con el objetivo de obtener los datos (logins, passwords, etc.) que permitirán al ladrón, acceder a cuentas bancarias accesibles a través de Internet.

Un software de tipo *crimeware* (generalmente un *troyano*) también podría conseguir redirigir el navegador web utilizado por el usuario, a una réplica del sitio web original, estando éste controlado por el ladrón. Esta redirección se podría dar incluso cuando el usuario teclee correctamente la URL del sitio web al que deseaba acceder, ya que si el troyano ha completado su trabajo, podría haber modificado el conjunto de direcciones DNS que asocian el nombre de dominio introducido por el usuario, con su dirección IP original. Ahora la información DNS contenida en la máquina infectada por el *crimeware*, indicará al navegador la dirección IP del sitio replicado y controlado por el ladrón.

Grayware es un tipo de programa maligno que involucra aquellos programas que se comportan de forma molesta o indeseada.

Los grayware abarcan otros tipos de malwares (programas malignos) como espías, adwares, dialers, etc. Grayware no incluye virus o troyanos.
Suelen afectar el rendimiento de la computadora. También a menudo los grayware suelen realizar acciones que son molestas para los usuarios, como ventanas pop-up con publicidad, entre otras.

Posibles problemas que acarrean los graywares:

- Reducción del rendimiento de la computadora.
- Incremento de los cuelgues en aplicaciones y errores fatales.
- Reducen la eficiencia del usuario.
- Degradan el ancho de banda de la red o de internet.
- Pueden producir pérdida de información.
- Pérdida de privacidad del usuario que emplea la computadora infectada.

Métodos de infección Malware

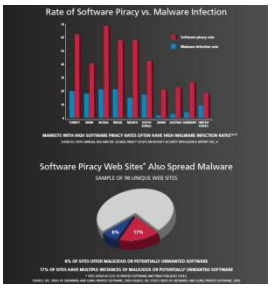
Entre los canales más usados por malware son:

- **Internet.** La red global es el origen principal de distribución de todos tipos de malware. En general, los virus y otros programas maliciosos se colocan en unas páginas Web populares pretendiéndose algún software útil y gratis. Muchos de los scripts que se ejecutan automáticamente al abrir las páginas Web también pueden contener programas maliciosos.

- **Correo electrónico**. Los emails en los buzones privados y las bases de correo pueden contener virus. Los archivos adjuntos y el cuerpo de email pueden contener malware. Los tipos principales de malware distribuido por correo electrónico son virus y gusanos. Puede infectar su equipo cuando abre un email o guarda un archivo adjunto. El correo electrónico es también un fuente de spam y phishing. Mientras spam es generalmente una pérdida de tiempo, phishing es un método de robar sus datos confidenciales (el número de su tarjeta de crédito, p.e.).

- **Vulnerabilidades de software**. Explotación de vulnerabilidades de software instalado en el sistema es el método preferido por los hackers. Las vulnerabilidades permiten a un hacker establecer una conexión remota a su equipo, y consecuentemente a sus datos, los datos de su red, etc.

- **Todos tipos de unidades de almacenamiento portátiles**. Discos externos, discos compactos y disquetes, unidades flash. Al conectar una unidad portátil a su equipo o iniciar algún archivo de allí, puede infectar su equipo con malware y empezar distribuirlo involuntariamente.



Explotación de vulnerabilidades

Existen varios factores que hacen a un sistema más vulnerable al malware: homogeneidad, errores de software, código sin confirmar, sobre-privilegios de usuario y sobre-privilegios de código.

Una causa de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. Por ejemplo, cuando todos los ordenadores de una red funcionan con el mismo sistema operativo, si se puede comprometer ese sistema, se podría afectar a cualquier ordenador que lo use. En particular, Microsoft Windows tiene la mayoría del mercado de los sistemas operativos, esto permite a los creadores de malware infectar una gran cantidad de computadoras sin tener que adaptar el software malicioso a diferentes sistemas operativos.

La mayoría del software y de los sistemas operativos contienen bugs que pueden ser aprovechados por el malware. Los ejemplos típicos son los desbordamiento de búfer (buffer overflow), en los cuales la estructura diseñada para almacenar datos en un área determinada de la memoria permite que sea ocupada por más datos de los que le caben, sobre escribiendo otras partes de la memoria. Esto puede ser utilizado por el malware para forzar al sistema a ejecutar su código malicioso.

Las memorias USB infectadas pueden dañar la computadora durante el arranque.

Originalmente las computadoras tenían que ser booteadas con un diskette, y hasta hace poco tiempo era común que fuera el dispositivo de arranque por defecto. Esto significaba que un diskette contaminado podía dañar la computadora durante el arranque, e igual se aplica a CD y memorias USB. Aunque eso es menos común ahora, sigue siendo posible olvidarse de que el equipo se inicia por defecto en un medio removible, y por seguridad normalmente no debería haber ningún diskette, CD, etc, al encender la computadora. Para solucionar este problema de seguridad basta con entrar en la BIOS del ordenador y cambiar el modo de arranque del ordenador.

Ingeniería Social

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de 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.

Propagación de malware a través de dispositivos USB

Los códigos maliciosos que se propagan a través de dispositivos USB son cada vez más comunes y todos tienen un funcionamiento similar.

La posibilidad de que el malware aproveche los avances tecnológicos para que a través de ellos se obtengan nuevos canales y medios de infección y propagación, constituye una de las tendencias de este y los próximos años.

Los dispositivos de almacenamiento siempre constituyeron una de las vías más comunes de infección, desde los viejos discos magnéticos de 5´1/4, pasando por los ya casi olvidados disquetes de 3´1/2 hasta llegar a los dispositivos de almacenamiento que permiten guardar información a través del puerto USB.

La natural evolución de la tecnología fue alimentando el crecimiento de las técnicas y metodologías de infección utilizadas por los desarrolladores de malware a través de sus creaciones maliciosas. La interconexión de redes de computadoras logró interacción a nivel mundial y, consecuentemente, la proliferación de nuevas técnicas de infección viral, cuya diseminación se produce casi en forma instantánea.

En lo particular, los medios de almacenamiento masivo a través de conexiones del tipo USB, como lo son los PenDriver (o flashdrive, memorias USB, etc.), representan un punto vulnerable para cualquier sistema informático. Debido a la masividad de uso y facilidad de conexión, se convierten en un medio común utilizado para transportar archivos y también todo tipo de malware.

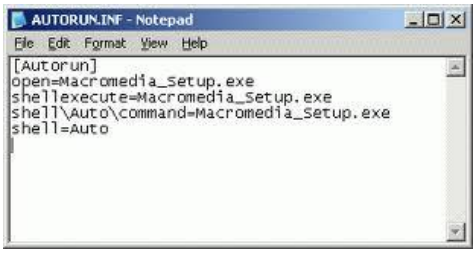
Los gusanos de Internet constituyen el principal tipo de programa dañino que comúnmente se aprovecha de estas características: la esencia de los gusanos informáticos es propagarse hacia la mayor cantidad de sistemas posibles copiando su propio código malicioso en cada infección, sin importar el medio por el cual lo haga.

Algunos ejemplos de malware que se diseminan aprovechándose de estos dispositivos son:

- **RJUMP:** este gusano posee características de troyano y abre una puerta trasera en el sistema infectado. Entre los medios de almacenamiento masivo que puede infectar se encuentran discos rígidos extraíbles, cámaras digitales y memorias USB.

- **Fujacks:** esta familia de gusanos no sólo se propaga a través de dispositivos de almacenamiento masivo sino que también infecta archivos ejecutables y recursos compartidos que existen en la red configurados con contraseñas débiles (o sin ellas).

- **AutoRun.C (también conocido como Zayle):** es un gusano de Internet que aprovecha la conexión a los dispositivos USB para propagarse e infectar las computadoras. Para lograr ejecutarse en forma automática, se vale de un archivo "autorun.inf". Además posee la capacidad de deshabilitar la opción de abrir las unidades con doble clic.



Tanto los códigos maliciosos mencionados como la mayoría del malware en general, utilizan formas comunes de infección; como por ejemplo, copiarse a sí mismo a un determinado sector del disco, manipular el registro de Windows, etc.

En el caso de las infecciones a través de dispositivos USB, el malware se vale de un archivo llamado "autorun.inf" que se encarga de ejecutar el código malicioso en forma automática cuando el dispositivo es insertado en la computadora. Esto sucede si el usuario no ha deshabilitado esta opción explícitamente (lo que la mayoría de los usuarios no hacemos) y que a continuación muestra la siguiente ventana:

Este es el comportamiento normal del sistema operativo al insertar un CD o dispositivo USB, del cual se vale el programa dañino para infectar el equipo.

Estos programas dañinos trabajan de la siguiente manera: al conectar el dispositivo en uno de los puertos USB el malware se ejecuta en forma automática (valiéndose del archivo mencionado) y se copia en distintas ubicaciones de los discos locales (generalmente con atributos de oculto/sistema), infectando de esta manera a cada uno de los dispositivos donde se lo inserta.

Asimismo, cada vez que un nuevo dispositivo de almacenamiento masivo es insertado en la computadora comprometida, el gusano se encargará de copiarse en el nuevo medio extraíble y así sucesivamente, infectando la máxima cantidad de dispositivos posibles.

Es importante que los usuarios tomen conciencia del peligro que representan los dispositivos de almacenamiento masivo como los mencionados, debido a la facilidad con la que pueden disparar infecciones de cualquier tipo de malware.

¿Qué son las cookies?

Las **cookies** son ficheros de texto que se crean al visitar una página web, y que **sirven para almacenar información** de diversos tipos que no debería afectar a tu privacidad. Por poner un ejemplo, gracias a las cookies se pueden guardar las preferencias de una página web o la contraseña y el nombre de usuario durante un determinado tiempo.
Sin embargo, algunas páginas web utilizan la información recogida en estas cookies para recopilar información del usuario y seguidamente enviarle publicidad, por lo que se consideran un tipo de spyware.

¿Cómo sé si un sitio tiene cookies maliciosas?

Cuando se navega por internet, se debe hacer de una manera responsable: **debe primar la desconfianza**. Generalmente, las páginas que aparentan tener un 'contenido de dudosa legalidad', **material pornográfico** e incluso que ofrecen descargas de programas de pago de forma gratuita, suelen ser los principales focos de cookies maliciosas, y es por ello que empresas como Google o Microsoft nos avisan si nos dirigimos desde sus buscadores a estos sitios de que podríamos estar en riesgo.

Además, los navegadores modernos, disponen de algoritmos para identificar este tipo de páginas, aunque no son ni mucho menos perfectos, por lo que no es recomendable fiarse al 100% de ellos.

¿Cómo configuro mi navegador para gestionar cookies?

Todos los navegadores actuales permiten **gestionar las cookies** a distintos niveles de seguridad. Por ejemplo, en Internet Explorer, se puede elegir el nivel de seguridad moviendo una barra deslizante. Cuanto más arriba esté dicha barra, mayor seguridad y privacidad tendremos, y, cuanto más abajo esté, más cookies y menos seguridad tendremos.

Aunque parezca lo contrario, **no siempre resulta mejor tener la barra deslizante en lo más alto**, ya que hay numerosas páginas web (Por ejemplo los bancos) que requieren tenerlas activadas.

Leyendas Urbanas de las cookies

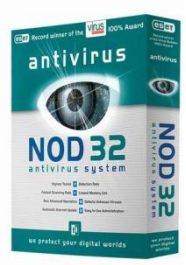
- Las cookies son similares a **gusanos** y virus en que pueden borrar datos de los discos duros de los usuarios.
- Las cookies son un tipo de **spyware** porque pueden leer información personal almacenada en el ordenador de los usuarios.
- Las cookies generan **popups**.
- Las cookies se utilizan para generar **spam**.
- Las cookies sólo se utilizan con **fines publicitarios**.

- **Herramientas paliativas. Instalación y configuración:**

Son una serie de herramientas que tratan de evitar cualquiera de los ataques informáticos que hemos estudiado en el apartado anterior.

- Software antimalware: Antivirus (escritorio, on line, portables, Live), Antispyware, Herramientas de bloqueo web.

Antivirus: Un **virus informático** es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.



¿Qué es un antivirus?
Aplicación o aplicaciones que previenen, detectan, buscan, y eliminan virus, utilizando bases de datos de nombres, y diversas técnicas heurísticas de detección.
La base fundamental de un programa antivirus es su capacidad de actualización de la base de datos. A mayor frecuencia de actualización, mejor protección contra nuevas amenazas.
Dentro de los antivirus encontramos diversas subcategorías: antivirus activo, antivirus pasivo, antivirus online, antivirus offline y antivirus gratuito.

Tipos de antivirus

Los programas antivirus pueden dividirse en 4 tipos :

Detectores: Detectan la presencia de virus conocidos y avisan al usuario para que tome medidas contra ellos. Este es el tipo de antivirus más simple.

Eliminadores/Reparadores: También conocidos como "mata-virus". Además de detectar la presencia de un virus, pueden eliminarlo de los ficheros contaminados o la zona de arranque del disco, dejando los programas ejecutables en su estado original. Esto no siempre es posible, ya ya que algunos virus sobreescriben parte del código original del programa infectado.

Protectores: También conocidos como "programas preventivos" o "inmunizadores". Se anticipan a la infección de cualquier virus, caballo de Troya o acción voluntaria involuntaria de destrucción de datos (por ejemplo, un FORMAT C:), permaneciendo residentes en la memoria del ordenador y vigilando las operaciones de ejecución de programa, copia ficheros, formateado de discos, etc. Suelen ser programas muy seguros que generalmente pueden detectar nuevos virus y evitar la acción de los caballos de Troya y bombas lógicas.

Programas de Vacuna: Añaden código a un fichero ejecutable de modo que éste se autochequee al ejecutarse, o calculan y guardan una lista de sumas de control en cierta parte del disco. Los programas de este tipo suelen presentar problemas de compatibilidad.

-Antivirus online Tipos:

Un antivirus en línea, es un programa antivirus que se ofrece, por lo general, de forma gratuita para "escanear" y en algunos casos desinfectar los archivos infectados por virus. La característica principal de este tipo de programa es que se distribuyen a través de Internet, basta con tener un navegador Web (Internet Explorer) y acceso a la red para poder utilizarlo.

-Antivirus de escritorio

Los antivirus de escritorio se suelen utilizar en modo residente para proteger al ordenador en todo momento de cualquier posible infección, ya sea al navegar por Internet, recibir algún correo infectado o introducir en el equipo algún dispositivo extraíble que esté infectado. No necesitan que el ordenador esté conectado a Internet para poder funcionar, pero sí que es necesario actualizarlos frecuentemente para que sean capaces de detectar las últimas amenazas de virus. Recomendamos tener sólo un antivirus de escritorio en el ordenador, ya que tener varios antivirus puede ocasionar problemas de incompatibilidad entre ellos.

-Antivirus Live CD

Muchas veces se meten virus en el Windows y son difíciles de quitar si estamos desde el mismo sistema infectado. Para solventarlo existen los Antivirus LiveCD, que son distribuciones de Linux, con un motor antivirus que se ejecutan desde el CD y por tanto no hay necesidad de instalar antivirus. Esto nos ayudará a limpiar nuestro Windows de virus, troyanos y otras bestias.

-Antispyware

El Spyware es software espía. Son programas que se instalan en su PC de modo automático o que vienen camuflados en la instalación de programas más respetables, es frecuente que en los programas freeware que uno instala, que los mismos tengan algún componente espía. Sin ir más lejos, la versión standard del Kazaa y otros programas de intercambios de archivos, los packs de emoticones para MSN Messenger y otros servicios de mensajería - que no sean los oficiales de Microsoft, por ejemplo -, bastantes programas aceleradores de downloads, juegos gratis, y en general todo caballo regalado que hay por Internet tiene un componente Spyware.

Aplicación que busca, detecta y elimina programas espías (spyware) que se instalan ocultamente en el ordenador.
Los antiespías pueden instalarse de manera separada o integrado con paquete de seguridad (que incluye antivirus, cortafuegos, etc).

-Herramientas de bloqueo web

Este tipo de programas limita el acceso en función de un listado de páginas negativas o positivas.

En el primer caso, listas negativas, se bloquean una serie de páginas por considerarlas ofensivas para los menores. El principal problema de estas listas es que pronto se quedan obsoletas debido a la rápida creación de nuevas páginas Web. Por ello, los productores de este tipo de filtros han optado por la configuración de listas positivas. Esto significa que cuando los niños navegan por Internet sólo pueden consultar las páginas incluidas en esta lista. Actualmente es una solución más eficaz y segura que las listas negativas y se ha acuñado el término ***"navegador infantil" (walled garden)*** para denominar a los programas que utilizan listas positivas.

Canguro Net

- **Herramientas preventivas. Instalación y configuración:**

Son una serie de herramientas que tratan de evitar cualquiera de los ataques informáticos que hemos estudiado en el apartado anterior y que Incluyen:

- Encriptado de información en disco
- Antivirus
- Sistemas de detección de intrusos (IDS)
- Sistemas de prevención de intrusos (IPS)
- Backup

Control de acceso lógico

Control de acceso lógico (política de contraseñas seguras, control de acceso en la BIOS y gestor de arranque, control de acceso en el sistema operativo, política de usuarios y grupos, actualización de sistemas y aplicaciones)
El acceso lógico incluye una serie de aplicaciones para PC y redes, incluyendo autentificación y/o acceso a la PC o red, email seguro, encriptación de datos, encriptación de archivo/carpetas, acceso remoto VPN, entre otros.

Medidas de control de acceso lógico:

Seguridad del BIOS y del gestor de arranque

La protección con contraseñas para el BIOS (o equivalentes al BIOS) y el gestor de arranque, pueden ayudar a prevenir que usuarios no autorizados que tengan acceso físico a sus sistemas, arranquen desde medios removibles u obtengan acceso como root a través del modo monousuario. Pero las medidas de seguridad que uno debería tomar para protegerse contra tales ataques dependen tanto de la confidencialidad de la información que las estaciones tengan como de la ubicación de la máquina.

Contraseñas del BIOS

Las siguientes son las dos razones básicas por las que proteger la BIOS de una computadora con una contraseña

1. *Prevenir cambios a las configuraciones del BIOS* — Si un intruso tiene acceso a la BIOS, puede configurarlo para que arranque desde un diskette o CD-ROM. Esto les permite entrar en modo de rescate o monousuario, lo que a su vez les permite plantar programas dañinos en el sistema o copiar datos confidenciales.

2. *Prevenir el arranque del sistema* — Algunas BIOSes le permiten proteger el proceso de arranque con una contraseña. Cuando está funcionalidad está activada, un atacante esta forzado a introducir una contraseña antes de que el BIOS lanze el gestor de arranque.

Si olvida su contraseña del BIOS, usualmente esta se puede reconfigurar bien sea a través de los jumpers en la tarjeta madre o desconectando la batería CMOS. Por esta razón, es una buena idea bloquear el chasis del computador si es posible. Sin embargo, consulte el manual del computador o tarjeta madre antes de proceder a desconectar la batería CMOS.

Contraseñas del gestor de arranque

A continuación se muestran las razones principales por las cuales proteger el gestor de arranque Linux:

1. *Previene el acceso en modo monousuario* — Si un atacante puede arrancar en modo monousuario, se convierte en el superusuario de forma automática sin que se le solicite la contraseña de acceso.
2. *Previene el acceso a la consola de GRUB* — Si la máquina utiliza GRUB como el gestor de arranque, un atacante puede usar la interfaz del editor para cambiar su configuración o para reunir información usando el comando cat.
3. *Previene el acceso a sistemas operativos inseguros* — Si es un sistema de arranque dual, un atacante puede seleccionar un sistema operativo en el momento de arranque, tal como DOS, el cual ignora los controles de acceso y los permisos de archivos.

.

Protegiendo GRUB con contraseñas

Puede configurar GRUB añadiendo una directiva de contraseña a su archivo de configuración. Para hacer esto, primero seleccione una contraseña, luego abra un indicador de comandos del shell, conéctese como root y escriba:

```
/sbin/grub-md5-crypt
```

Cuando se le pida, escriba la contraseña GRUB y presione [Intro]. Esto retornará un hash MD5 para la contraseña.

Luego, modifique el archivo de configuración GRUB /boot/grub/grub.conf. Abra el archivo y debajo de la línea timeout en la sección principal del documento, añada la siguiente línea:

```
password --md5 <password-hash>
```

Reempace *<password-hash>* con el valor retornado por /sbin/grub-md5-crypt

La próxima vez que el sistema arranque, el menú de GRUB no le permitirá accesar el editor o la interfaz de comandos sin primero presionar [p] seguido por la contraseña de GRUB.

Lamentablemente, esta solución no previene a un atacante de arrancar en un sistema operativo inseguro, si se está en un ambiente de arranque dual. Para esto, necesita editar una parte diferente del archivo /boot/grub/grub.conf.

Busque la línea title del sistema operativo inseguro y añada una línea que diga lock directamente debajo de ella.

Para un sistema DOS, la estrofa debería comenzar con algo similar a:

```
title DOS
lock
```

Para crear una contraseña diferente para un kernel o sistema operativo particular, añada una línea lock a la estrofa, seguido por una línea de contraseña.

Cada estrofa que usted proteja con una contraseña única debería comenzar con líneas similares a las del ejemplo siguiente:

```
title DOS
lock
password --md5 <password-hash>
```

CONTROL DE ACCESO AL SISTEMA OPERATIVO

Objetivo: evitar el acceso no autorizado a los sistemas operativos. Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:
a) autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;
b) registrar intentos exitosos y fallidos de autenticación del sistema;
c) registrar el uso de privilegios especiales del sistema;
d) emitir alarmas cuando se violan las políticas de seguridad del sistema;
e) suministrar medios adecuados para la autenticación;
f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

Configurar la seguridad de usuarios y grupos

Configurar la seguridad de usuarios y grupos

Para proteger un equipo y sus recursos, debe decidir qué tareas y acciones pueden realizar los usuarios o grupos de usuarios. Las tareas y acciones que un usuario o un grupo de usuarios pueden realizar dependen de los derechos de usuario que les asigne. Por ejemplo, si un miembro de confianza del grupo Usuarios necesita supervisar el registro de seguridad, puede concederle el derecho "Administrar auditoría y registro de seguridad" en lugar de agregar el usuario a un grupo con más privilegios, como el grupo Administradores. De la misma forma, puede proteger un objeto, como un archivo o una carpeta, si asigna permisos.

Algunas de las tareas más comunes son asignar derechos de usuario en el equipo local, asignar derechos de usuario en toda la organización y establecer permisos de archivos y carpetas. Para obtener más información acerca de otras tareas para configurar la seguridad de usuarios y grupos, vea Procedimientos de control de acceso.

ACTUALIZACIONES DE SW Y SO

Necesidad de las actualizaciones

Mientras hacemos uso de Internet y sus servicios, los ciberdelincuentes- de forma análoga a como haría un ladrón al intentar entrar a robar a una casa– desarrollan software malicioso para aprovechar cualquier vulnerabilidad en el sistema a través del cual infectarlo. Suelen aprovechar las vulnerabilidades más recientes que tienen tanto el sistema operativo como los demás programas, y que requieren una actualización inmediata de los sistemas.

Hay que tener en cuenta que cuanto más tiempo tardemos en actualizar nuestros equipos más tiempo estaremos expuestos a que cualquier tipo de malware pueda explotar alguna vulnerabilidad y nuestro equipo quede bajo el control del atacante.

Para facilitar esta tarea, la mayoría de aplicaciones y sistemas operativos tienen la opción de actualizar el sistema automáticamente, lo que permite tener los programas actualizados sin la necesidad de comprobar manual y periódicamente si la versión utilizada es la última disponible, y por tanto la más segura.

Estas actualizaciones de software vienen justificadas por diferentes motivos:

- Corregir las vulnerabilidades detectadas.
- Proporcionar nuevas funcionalidades o mejoras respecto a las versiones anteriores.

Aunque es posible hacer la actualización de forma manual, lo más sencillo es hacerlo de forma automática. De esta forma el propio sistema busca las actualizaciones, las descarga e instala sin que nosotros tengamos que intervenir en el proceso.

-ACTUALIZACIONES EN LOS SO

Generalmente los sistemas operativos vienen configurados de forma predeterminada con la opción de "Actualizaciones Automáticas" por lo que no es necesario habilitarla manualmente.

A continuación se explicarán donde y como se activan estas directivas de seguridad en los sistemas operativos más comunes.

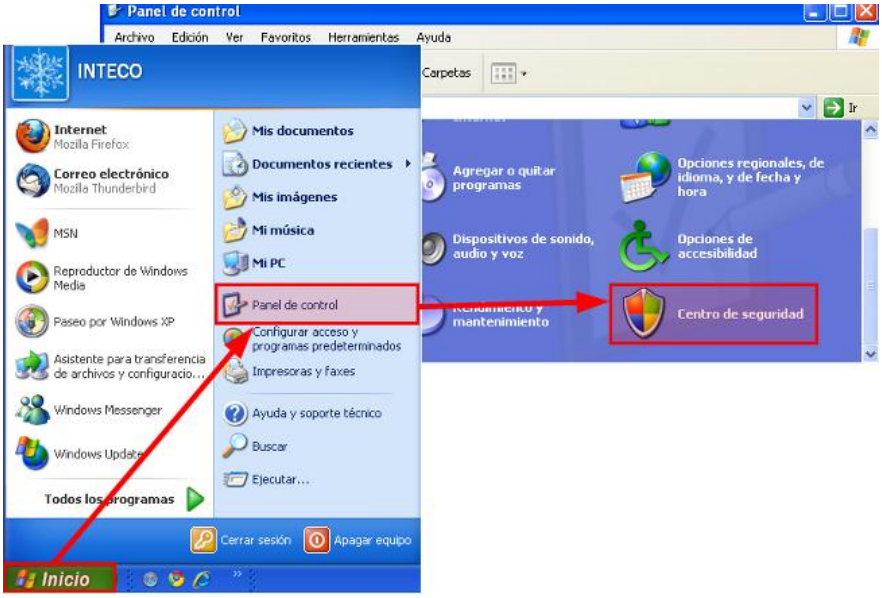
Microsoft

El ciclo habitual de actualizaciones de Microsoft se realiza los segundos martes de cada mes, salvo casos en los que el problema sea crítico y requiera de una actualización más inminente; este es uno de los motivos por el que se desaconseja totalmente no tener las actualizaciones autómaticas habilitadas ya que nuestro equipo podría encontrarse desprotegido en situaciones en las que se liberara un 0-day.
Las actualizaciones no interferirán con otras descargas y se descargarán de forma transparente al usuario siempre y cuando esté conectado a Internet.

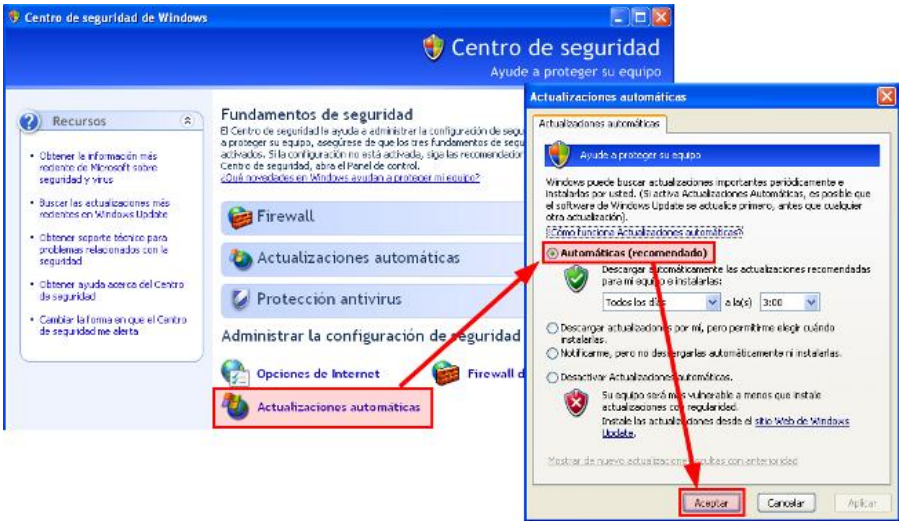
Para comprobar que tenemos configurado nuestro equipo correctamente siga los siguientes pasos.

- **WindowsXP:**

- Haga clic en "Inicio" → "Panel de control" → "Centro de seguridad"

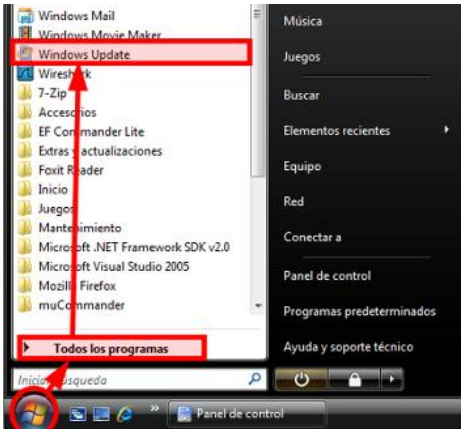


- Haga clic en → "Actualizaciones automáticas". Seleccione la opción "Automáticas (recomendado)"→ haga clic en el botón "Aceptar"

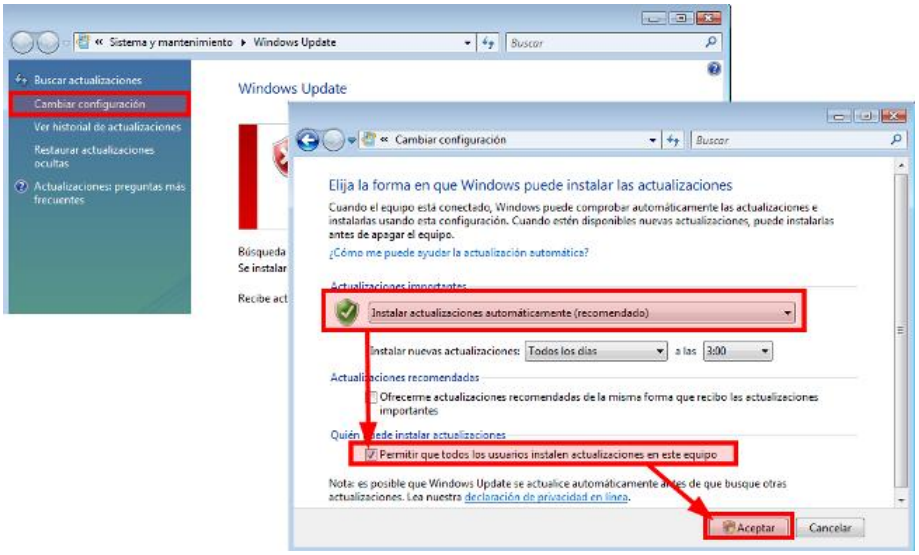


Windows **Vista:**

- Pulse en "Inicio" → "Todos los programas" → "Windows Update".

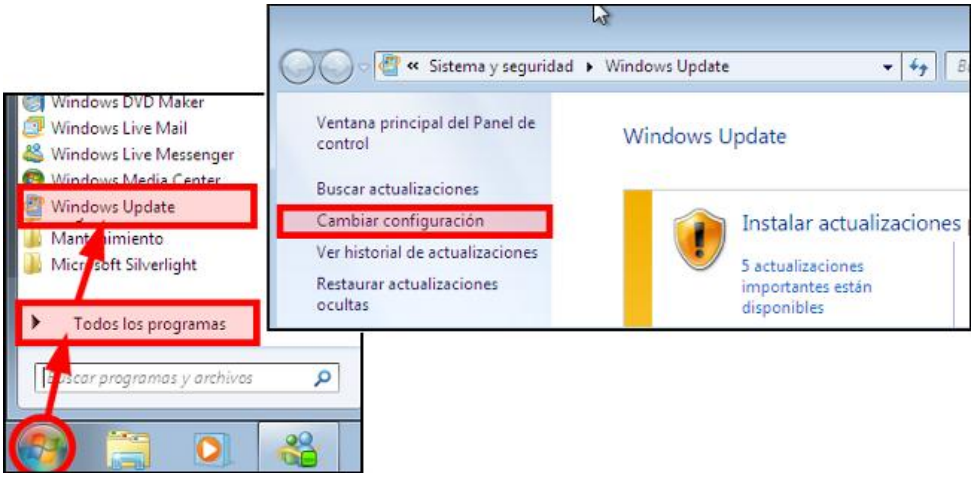


- En el panel izquierdo seleccione la opción “Cambiar la configuración” y posteriormente “Instalar actualizaciones automáticamente (recomendado)”, además se debe marcar la casilla de verificación “Permitir que todos los usuarios instalen actualizaciones en este equipo”. Por último haga clic en el botón «Aceptar»

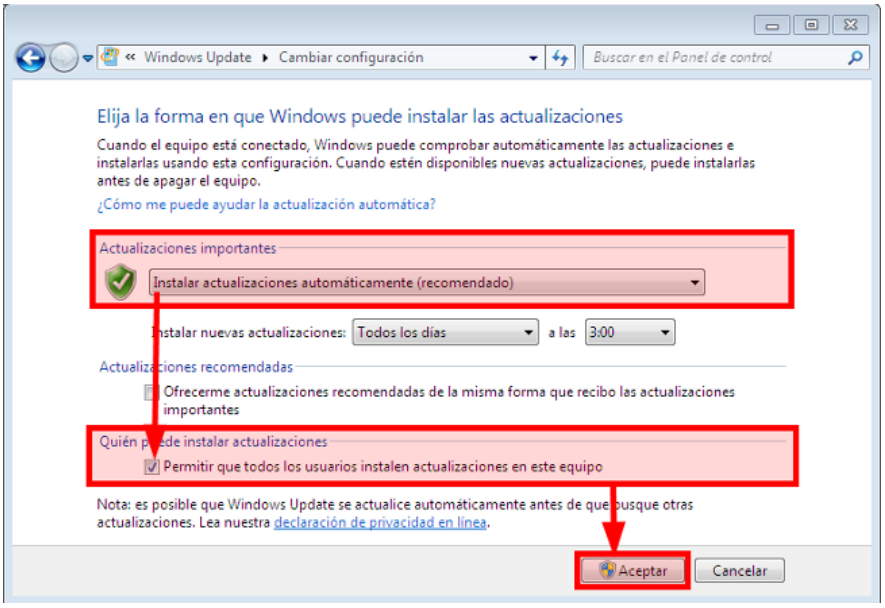


Windows **7:**

- Pulse en “Inicio” → “Todos los programas”-> “Windows Update” , en el panel izquierdo, pulse en “Cambiar la configuración.”



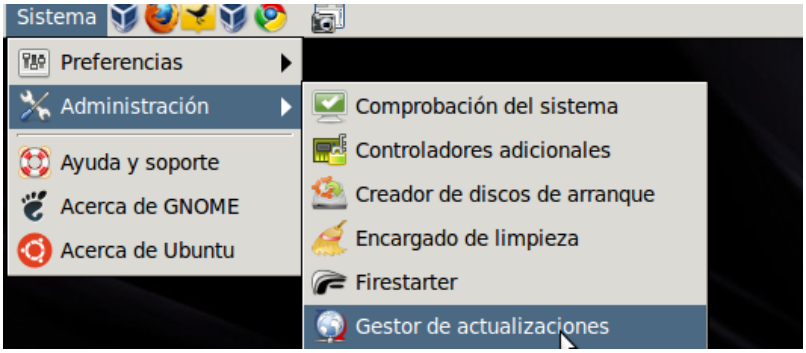
- Del desplegable de "Actualizaciones importantes", seleccione "Instalar actualizaciones automáticamente (recomendado)", se marcará la opción "Permitir que todos los usuarios instalen actualizaciones en este equipo". Por último, hacer clic en el botón «Aceptar»



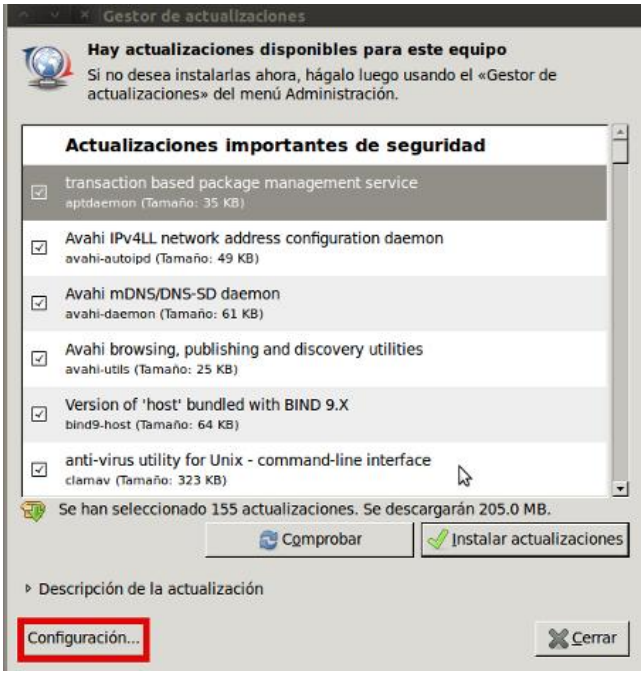
Ubuntu

Ubuntu también permite configurar actualizaciones automáticamente sin intervención del usuario o bien comprobar manualmente las actualizaciones disponibles. Para ello se seguirán los siguientes pasos:

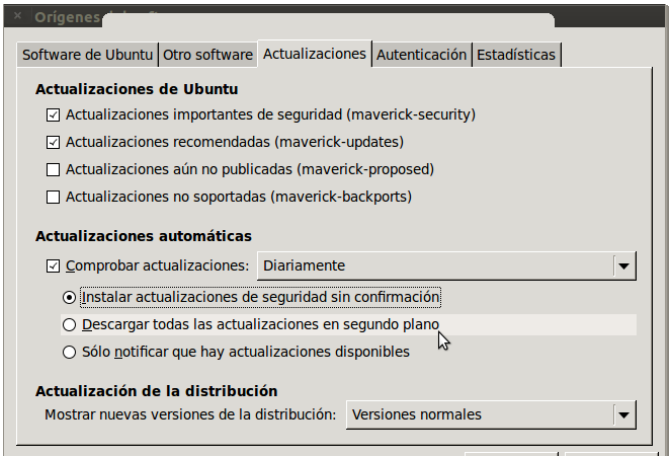
1. La configuración de las actualizaciones se encuentra en " Sistema" → "Administración" → "Gestor de Actualizaciones."



2. La ventana nos mostrará la opción de comprobar manualmente si existen actualizaciones y en caso de ser así instalarlas (botón "Instalar Actualizaciones").



3. Desde aquí también podremos acceder a la configuración de las actualizaciones mediante el botón "Configuración", desde donde podremos seleccionar el tipo de actualizaciones (importantes, recomendadas, aún no publicadas, no soportadas), el intervalo de las mismas (diariamente, semanalmente, etc) y si deseamos instalar las actualizaciones de seguridad sin confirmación (opción recomendada) o bien manualmente.



Las actualizaciones importantes de seguridad y actualizaciones recomendadas solucionan problemas de seguridad críticos y actualizan aplicaciones y módulos del Sistema Operativo, por lo que se recomienda que estén activadas.

Actualizaciones de la distribución:
Además de las actualizaciones de determinados programas y las actualizaciones circunstanciales que solventan problemas de seguridad, Ubuntu publica una versión estable de la distribución cada 6 meses proporcionando cambios importantes mediante la instalación de nuevos paquetes y actualizaciones para los componentes de nuestro sistema operativo. Además, Canonical proporciona soporte técnico y actualizaciones de seguridad durante 18 meses excepto para las versiones Long Term Support (versiones que se liberan cada cuatro versiones de Ubuntu) a las que proporcionan tres años para la versión de escritorio y cinco para la versión servidor.

Cuando exista una versión disponible para descargar, el gestor de actualizaciones nos avisará con un mensaje del siguiente tipo:

-ACTUALIZACIONES SW

Dale a tu sistema la mejor protección para que puedas hacer frente a los nuevos virus y amenazas. Instalando las actualizaciones que publican los fabricantes, conseguiremos estar mucho más seguros al navegar por la red de una manera rápida y cómoda.

Introducción

Cuando un desarrollador/fabricante publica un programa (sistema operativo, lector de documentos, reproductor de vídeo, etc.) pueden aparecen fallos de seguridad. Estos fallos de seguridad, a los que denominaremos vulnerabilidades, son aprovechados por los cibercriminales para tratar de infectar nuestro equipo con software malicioso para robar nuestros datos, usar nuestro equipo para su «trabajo», etc. Desde INTECO-CERT siempre hemos hecho hincapié en la constante atención sobre las actualizaciones de nuestro sistema operativo así como aquellos programas que puedan implicar un agujero de seguridad en caso de ser explotados por un atacante o cualquier tipo de malware. No seguir estas recomendaciones es temerario, lo mismo que otra serie de acciones por parte del usuario como son: el uso de cuentas privilegiadas, abrir ficheros adjuntos o URL de fuentes desconocidas, carecer de un Firewall o de Antivirus que nos avise de acciones sospechosas, etc.

- **Seguridad en la conexión con redes públicas:**

Uno de los peligros de estas redes es la captación de paquetes en las conexiónes mediante programas conocidos como "snifers", donde se puede extraer gran cantidad de información de las conexiónes como contraseñas o conversaciónes privadas entre otros datos. Para evitar este tipo de situaciones debemos usar un determinado tipo de claves, con técnicas de cifrado adecuados para evitar algunos tipos de ataques. También en algunos casos, debemos confirmar nuestra entidad.

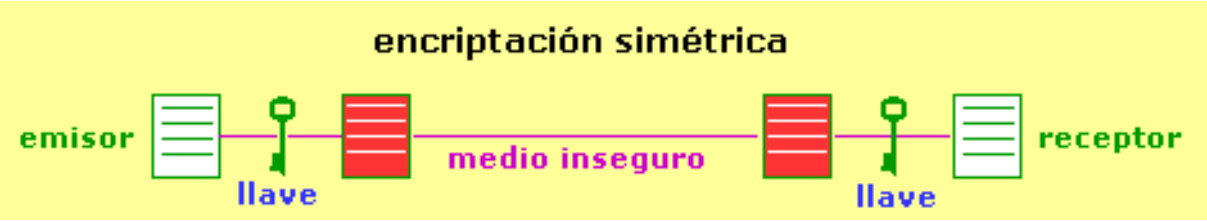
Técnicas de cifrado

Una técnica de cifrado es una operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro que permitirá obtener un texto cifrado y viceversa, garantizando la confidencialidad e integridad de la información contenida.
El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado. Las claves generalmente se dividen en:

- **Criptografía simétrica:**

Este tipo de criptografía, utiliza una única clave para cifrar y descifrar la información. Es el sistema más clásico de cifrado. Un ejemplo de este tipo de cifrado es el de las máquinas ENIGMA, utilizadas por los alemanes para cifrar sus comunicaciones durante la Segunda Guerra Mundial.

Su principal deficiencia reside en el hecho de que sólo existe una clave para convertir el texto en claro en criptograma y viceversa, lo que implica que ésta tiene que ser conocida por las dos partes que quieren intercambiar la información.



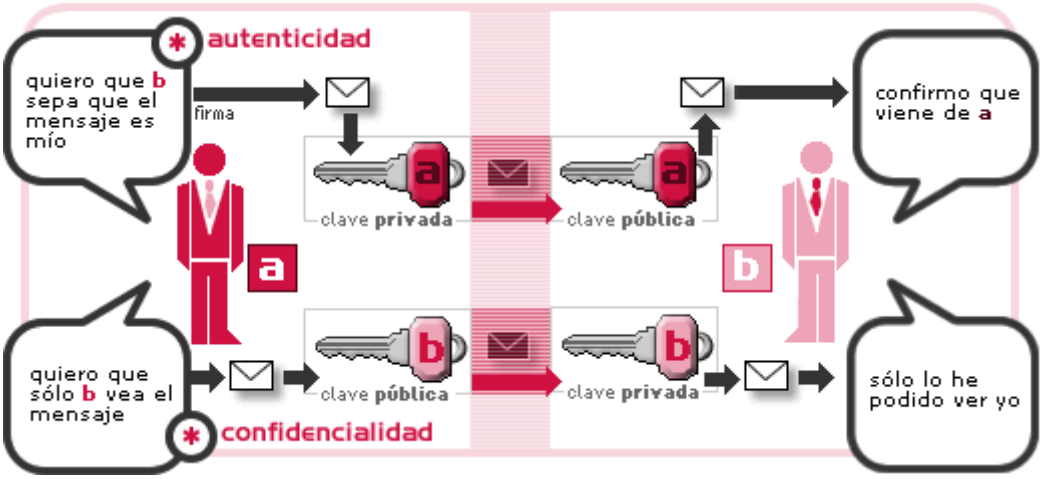
Desde el punto de vista de la seguridad de la información esto supone un importante riesgo sobre la fiabilidad de la confidencialidad otorgada por este tipo de sistemas criptográficos.

Algunos de los sistemas criptográficos simétricos más conocidos:

- **International Data Encryption Algorithm (IDEA)**.
- **Data Encryption Standard (DES/ Triple DES)**.
- **Advanced Encription Standard (AES)**

- **Criptografía asimétrica:**

Se conoce como criptografía asimétrica o de clave pública al sistema de encriptación que consiste en utilizar un sistema de doble clave: Clave Pública y Clave Privada. Una de ellas, la conocida como Clave Pública, es conocida por todos y se utiliza para convertir el Texto en Claro que queremos cifrar en un Criptograma, que tan solo podrá volverse a convertir en un Texto en Claro mediante la Clave Privada, conocida solamente por la persona a la que va remitida la información cifrada mediante la Clave Pública.



La principal ventaja que ofrece este sistema es que permite mantener en secreto la clave utilizada para descifrar el criptograma, lo cual implica que en ningún caso una información cifrada podrá ser pasada a Texto en Claro.
El problema de las claves asimétricas es que cuando el texto a tratar es largo el proceso de codificación es muy lento

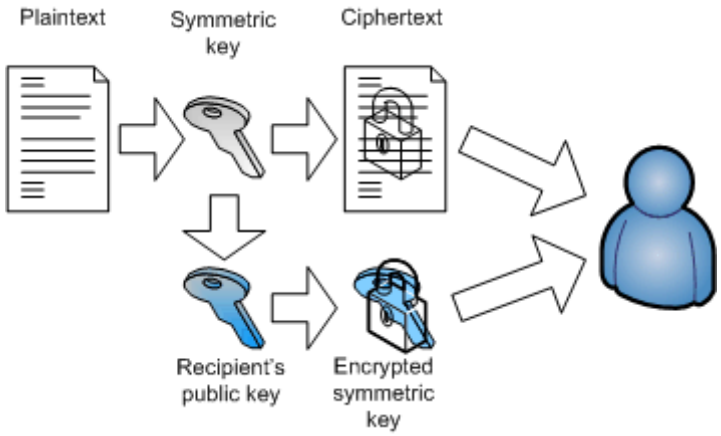
Los sistemas de criptografía asimétrica más conocidos son los siguientes:

- **RSA**: desarrollado originalmente en 1978 por R. Rivest, A. Shamir, L. Adleman, es uno de los más conocidos y sin duda el más actualizado actualmente.
- **Diffie-Hellman**: Este sistema recibe su nombre por sus creadores Whitfield Diffie y Martin Hellman.
- **CCE:** La conocida como criptografía de curva elíptica es un sistema más moderno y menos utilizado que los anteriormente citados, pero tal vez más eficiente a la hora de manejar más información.

- **Criptografía híbrida:**

La **criptografía híbrida** es un método criptográfico que usa tanto un cifrado simétrico como un asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión.

Tanto PGP como GnuPG usan sistemas de cifrado híbridos. La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.



Un sistema de cifrado híbrido no es más fuerte que el de cifrado asimétrico o el de cifrado simétrico de los que hace uso, independientemente de cuál sea más débil. En PGP y GnuPG el sistema de clave simétrica es probablemente la parte más débil de la combinación. Sin embargo, si un atacante pudiera descifrar una clave de sesión, sólo sería útil para poder leer un mensaje, el cifrado con esa clave de sesión. El atacante tendría que volver a empezar y descifrar otra clave de sesión para poder leer cualquier otro mensaje.

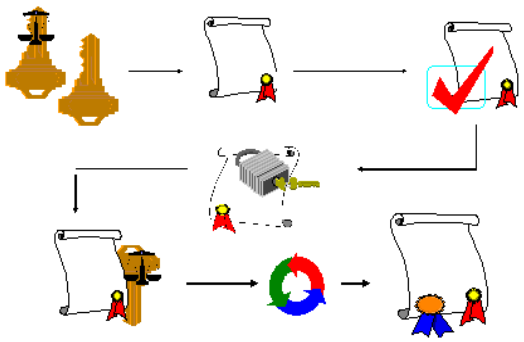
Identificación Digital:

Es aquel conjunto de rasgos propios de un individuo o colectividad que los caracterizan frente a los demás. La verificación de estos rasgos es lo que nos permite determinar que un individuo es quien dice ser. Algunos de estos rasgos son propios del individuo, otros son adquiridos con el tiempo. Por supuesto, no todos los rasgos son igualmente apreciables. Hay rasgos que son apreciables a simple vista, mientras que otros están ocultos y es necesario un conocimiento y, en ocasiones, herramientas para poder verificarlos.

Al **conjunto de rasgos que caracterizan a un individuo o colectivo en un medio de transmisión digital** se le conoce como ***Identidad Digital.***

- **Firma Electrónica y Firma Digital.**

  - **Firma Digital:** Se dice **firma digital** a un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión. Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.



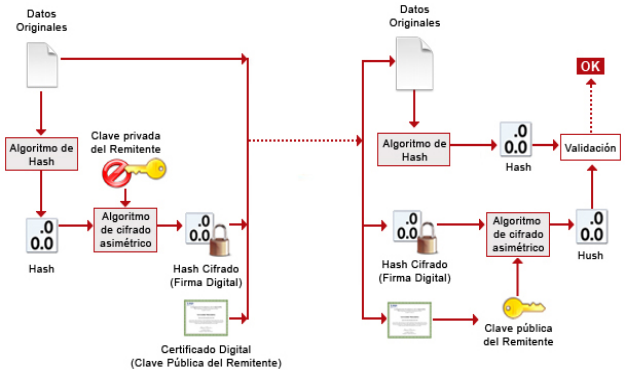
Consiste en un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante,
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- Inclusión de sello de tiempo.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. Ello no obstante, este tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

- **Firma Electrónica:** La **firma electrónica** es un concepto directamente relacionado con la firma digital, sin embargo no son lo mismo, a pesar del extendido uso indistinto y de una utilización léxica y práctica muy similar de estos dos conceptos. A pesar del uso indistinto que se le suele dar a los dos términos, entre los profesionales y expertos del tema se hace una clara diferenciación entre estos.



Una firma electrónica es una firma digital que se ha almacenado en un soporte de hardware; mientras que la firma digital se puede almacenar tanto en soportes de hardware como de software. La firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita.

De hecho se podría decir que una firma electrónica es una firma digital contenida o almacenada en un contenedor electrónico, normalmente un chip de ROM. Su principal característica diferenciadora con la firma digital es su cualidad de ser inmodificable (que no inviolable). No se debe confundir el almacenamiento en hardware, como por ejemplo, en un chip, con el almacenamiento de la firma digital en soportes físicos; es posible almacenar una firma digital en una memoria flash, pero al ser esta del tipo

RAM y no ROM, no se consideraría una firma electrónica si no una firma digital contenida en un soporte físico.

La firma digital contenida en soportes de tipo ROM tiene un uso muy extendido y se utiliza en gran cantidad de tarjetas de acceso, tarjetas de telefonía, RFID y otras actividades en la que es precisa identificar inequívocamente una persona u objeto.

Una aplicación destacada es el DNI electrónico español, también conocido como DNIE que al ser de uso obligado dispone de varios millones de usuarios.

Las características y usos de la Firma electrónica son exactamente los mismos que los de la Firma digital con la única diferenciación del tipo de soporte en el que se almacenan. Su condición de inmodificable aporta un grado superior de seguridad, si bien la ausencia habitual de contraseñas de seguridad que protejan su uso permitiría que un portador ilegítimo pudiese suplantar al propietario con facilidad.

- **Certificado digital, Autoridad Certificadora (CA)**

  - **Certificado Digital:** Un certificado digital, también llamado certificado de clave pública, es un documento electrónico que usa una firma electrónica para atestiguar que una clave pública pertenece a una persona u organismo concreto.

    Un aspecto fundamental que hay que entender es que el certificado para cumplir la función de identificación y autenticación necesita del uso de la clave privada (que sólo el titular conoce). El certificado y la clave pública se consideran información no sensible que puede distribuirse perfectamente a terceros. Por tanto el certificado sin más no puede ser utilizado como medio de identificación, pero es pieza imprescindible en los protocolos usados para autenticar a las partes de una comunicación digital, al garantizar la relación entre una clave pública y una identidad.

    El **certificado** debe contener al menos lo siguiente:

    - La identidad del propietario del certificado (identidad a certificar),
    - La clave pública asociada a esa identidad,
    - La identidad de la entidad que expide y firma el certificado,
    - El algoritmo criptográfico usado para firmar el certificado.

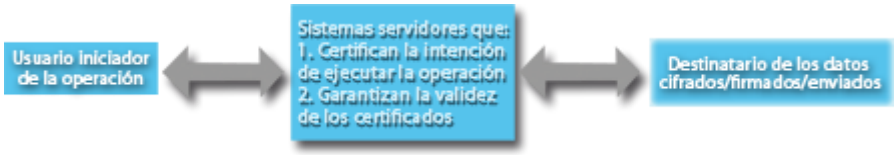
  - **Autoridad Certificadora:** La **Autoridad de Certificación** (AC o CA, según las siglas de *Certification Authority*), es la entidad que garantiza la autenticidad y veracidad de los datos recogidos en el certificado digital expedido. Se trata de una suerte de institución notarial que ofrece fidelidad a un hecho jurídico.

    El procedimiento de la Autoridad de Certificación se produce gracias a la posesión y utilización de una clave privada que garantiza la identidad del propietario del certificado digital. Esto provoca la posibilidad de firmar electrónicamente los certificados emitidos.
    Por otra parte, la Autoridad de certificación ofrece el servicio de **verificación de validez de los certificados**, ya que estos pueden ser revocados (pueden perder su validez por caducidad o sanción).

La emisión de certificados puede realizarse a personas y empresas, así como a Autoridades de Certificación de menor rango, estableciéndose una jerarquía de emisión de certificados. La estructura se organiza en función de una Autoridad de Certificación auto-firmada (convirtiéndose en la CA raíz). El certificado de la última Autoridad de Certificación es avalado, para asegurar su autenticidad, mediante su instalación en un almacén de certificados del propio ordenador, que luego usarán los navegadores. Así, se descarga el certificado raíz de la Autoridad de Certificación desde su sitio Web, ofreciendo confianza en la seguridad que ofrece su propia página.

Un concepto esencial para la comprensión de las Autoridades de Certificación es el de **infraestructura de clave pública** o, según sus siglas en inglés, **PKI** (***P**ublic **K**ey **I**nfrastructure*). PKI es una combinación de software y hardware, políticas y procedimientos de seguridad que permiten ejecutar operaciones criptográficas, como el cifrado, la firma digital o el no repudio de transacciones electrónicas, con las garantías necesarias.

Las partes que intervienen cuando se usa infraestructuras PKI son:



- **Documento Nacional de Identidad Electrónico (DNIe)**

Definición

El Documento Nacional de Identidad electrónico es el documento que acredita física y digitalmente la identidad personal de su titular y permite la firma electrónica de documentos.

¿Qué ventajas tiene respecto del DNI convencional?

Además de identificar al usuario ante terceros, permite la firma electrónica. El nuevo DNI aporta seguridad, rapidez, comodidad y la inmediata realización de trámites administrativos y comerciales a través de medios telemáticos.

¿Quién expide el DNI electrónico?

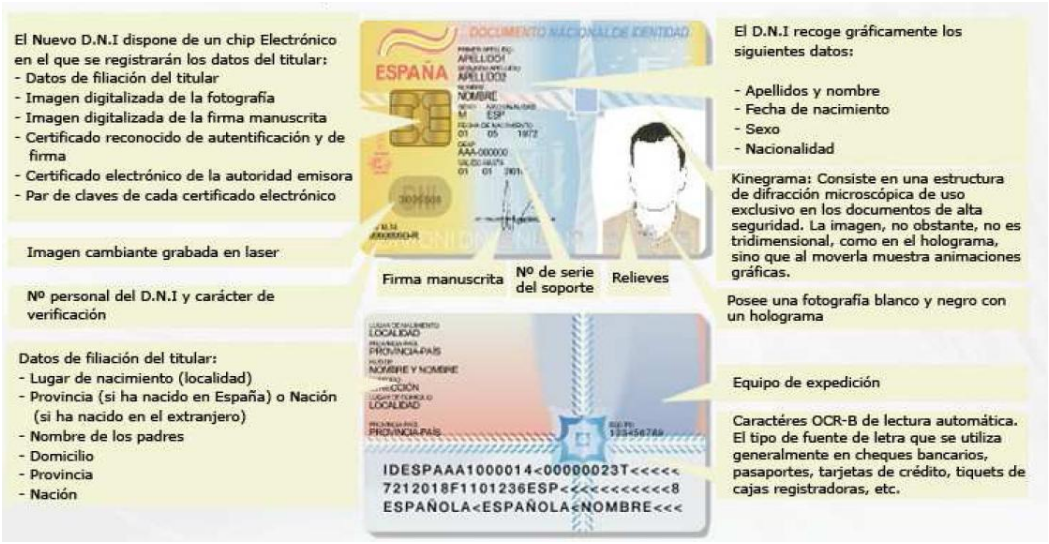
La Dirección General de la Policía es el único organismo autorizado a emitir los certificados digitales para el DNI electrónico. Los procedimientos de solicitud, revocación, renovación y período de vigencia de los certificados están regulados en la Política de Certificación.

¿Cuáles son sus posibles usos?

El tipo de usos es enorme. En principio la utilización del DNI electrónico es válida para todo tipo de tramitación telemática: desde solicitar una beca a presentar la Declaración de la Renta y otros impuestos o acceder a los datos de la Seguridad Social, así como el acceso a información personal en bases de datos públicas, la realización de transacciones con empresas, etc.

Descripción Física del DNI-e

Su **apariencia es similar al DNI actual**, al que se incorpora un **chip electrónico**, que contiene la información básica que permita acreditar electrónicamente **la identidad** de su titular **y la firma** de documentos electrónicos con plena validez legal.



Elementos de Seguridad Tarjeta Soporte

El DNI-e se compone de una tarjeta de policarbonato, a la que se han añadido diferentes **elementos de seguridad contra la falsificación**, e incorpora un chip criptográfico.

El DNI electrónico es un documento **más seguro que el tradicional**, pues incorpora mayores y **más sofisticadas medidas de seguridad** que harán virtualmente imposible su falsificación.

Utilidad del DNI-e

Se ofrecen a los ciudadanos y pymes, herramientas de fácil manejo para que, con su utilización, se fomente el uso de DNI electrónico. Estas herramientas pueden

- Aplicación de firma electrónica.
- Catálogo de sitios web donde se permite la utilización del DNI electrónico.
- Gestión de las consultas e incidencias sobre DNI-e, firma electrónica, tecnología y soluciones, que se reporten al CERT de INTECO.
- Adaptación del propio Portal de INTECO al uso del DNI-e.

Qué hace falta para utilizarlo

Una vez que haya obtenido su **DNI electrónico** necesitará adquirir el **lector DNI**. Existen diferentes modelos tanto para PC de sobremesa como portátil. Los modelos USB y Teclado multimedia pueden usarse en cualquier PC o portátil que tenga un puerto USB libre. El modelo PCMCIA está diseñado para ser usado en portátiles y su ventaja principal es la de permanecer insertado dentro del portátil sin tener que cargar con un dispositivo externo más. De una forma similar el **lector DNI** de bahía está pensado para su instalación en una bahía de 3.5" del PC sobremesa. Este último *lector de tarjetas* es especialmente útil cuando el puesto de trabajo se encuentra en lugares de acceso público.

Existen unos requisitos mínimos tanto para el PC donde vaya a ser usado el dnie como para la tecnología usada por el **lector de DNI**.

El ordenador personal debe al menos un Intel Pentium III o tecnología similar.
El lector de tarjetas debe cumplir los siguientes requisitos:

- Cumpla el estándar ISO 7816 (1, 2 y 3).
- Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1).
- Soporta velocidades de comunicación mínimas de 9.600 bps.
- Soporta los estándares
  - API PC/SC (Personal Computer/Smart Card)
  - CSP (Cryptographic Service Provider, Microsoft)
  - API PKCS#11

- **Buenas prácticas en el uso del certificado digital y DNIe.**

Pérdida o sustracción del documento

En caso de pérdida o sustracción del DNI electrónico, el titular deberá comunicarlos a la Dirección General de la Policía o de la Guardia Civil, bien denunciándolo en cualquier Comisaría de Policía o Puesto de la Guardia Civil, bien solicitando un duplicado del mismo en el equipo de expedición

Una vez en la Oficina de Expedición, en determinadas circunstancias deberá cumplimentar un impreso que le será entregado en la propia oficina y si el DNI extraviado o sustraído era del modelo anterior deberá aportar una fotografía más que junto a su firma y su impresión dactilar, servirá de comprobación de su identidad. Igualmente, se generarán nuevas claves y se expedirán nuevos certificados electrónicos**.**

Custodia de las claves privadas de los Certificados

La custodia de las claves privadas de los Certificados de Identidad Pública la realizan los ciudadanos titulares de las mismas. En ningún caso la Autoridad de Certificación guarda copia de la clave privada ya que ésta no puede ser extraída de la tarjeta.

Las claves privadas del ciudadano se encuentran almacenadas en el procesador de la tarjeta criptográfica del DNI electrónico. Con esto se consigue que las claves privadas no abandonen nunca el soporte físico del DNI, minimizando las posibilidades de poner en riesgo dichas claves.

Para el acceso a las claves y al certificado de firma el ciudadano deberá emplear una clave personal de acceso (PIN) generada en el momento de recibir su DNI electrónico y que sólo él debe conocer.

En todo momento el ciudadano podrá modificar la clave personal de acceso en una Oficina de Expedición utilizando los puestos destinados a tal efecto (Puntos de Actualización del DNI electrónico) y mediante el siguiente procedimiento:

- Si conoce la clave personal de acceso – PIN - podrá emplearlo durante el proceso de cambio.
- En caso de no recordar la clave personal de acceso – PIN - (o encontrase bloqueada la tarjeta al superar el número de **tres** intentos con un PIN incorrecto) podrá realizar el cambio mediante la comprobación de la biometría de impresión dactilar.

En ningún caso el olvido de la clave personal de acceso supondrá la revocación de los Certificados de Identidad Pública, siempre que pueda ser modificada por el procedimiento anterior.
También se habilitará un procedimiento telemático que permitirá el cambio de la clave personal de acceso – PIN - siempre que se recuerde el PIN vigente. En caso de no recordar la clave personal de acceso -PIN- (o encontrarse bloqueada la tarjeta al superar el número de tres intentos con un PIN incorrecto), sólo podrá realizar el cambio mediante la comprobación de la impresión dactilar en un Punto de Actualización del DNIe situado en las oficinas de expedición.

Algunas recomendaciones sobre la clave personal de acceso (PIN)

El PIN es una clave confidencial, personal e intransferible y es el parámetro que protege la clave privada de firma y permite activarlas en las aplicaciones que generan firma electrónica; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:

- Memorícelo y procure no anotarlo en ningún documento físico ni electrónico que el Titular conserve o transporte junto con la tarjeta del DNI electrónico, fundamentalmente si existe posibilidad de que se pierda o se robe al mismo tiempo que aquella.

- No envíe ni comunique su PIN a nadie ni por ningún medio, ya sea vía telefónica, correo electrónico, etc.

- Recuerde que el PIN es personal e intransferible. Si cree que su PIN puede ser conocido por otra persona, debe cambiarlo. El hecho de que el PIN sea conocido por una persona distinta supone un riesgo importante, ya que permite la activación de las claves privadas para poder realizar operaciones de firma electrónica en su nombre. Es obligación del titular notificar la pérdida de control sobre su clave privada, a causa del compromiso del PIN, ya que es motivo de revocación del certificado asociado a dichas claves.

- Como consejo adicional, evite escoger un número relacionado con sus datos personales, así como cualquier otro código que pueda resultar fácilmente predecible por terceras personas (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones de la misma cifra, secuencias de cifras que ya forman parte de su número de DNI electrónico, etc.)

- Se recomienda cambiarlo periódicamente.

- **Amenazas y ataques en redes corporativas:**

Amenaza interna o corporativa y Amenaza externa o de acceso remoto.

Algunas razones *por qué los atacantes de la red tratan de atacar a las redes corporativas* se enumeran aquí:

- Los individuos que buscan la fama o algún tipo de reconocimiento. "script kiddies" por lo general buscan alguna forma de la fama cuando intentan accidente sitios Web y otros objetivos públicos en Internet. Un script kiddie también podría estar buscando alguna forma de aceptación o reconocimiento por parte de la comunidad de hackers o piratas informáticos de sombrero negro.

- los motivos posibles de las amenazas externas estructuradas incluyen:
  - Codicia
  - Espionaje industrial
  - Política
  - Terrorismo
  - Racismo
  - Penal pagos

- Enfadado empleados podrían tratar de dañar los datos de la organización, la fiabilidad o la capacidad financiera.

- Existen, sin embargo algunos atacantes de red que simplemente disfrutar el desafío de tratar de poner en peligro los sistemas de seguridad de las redes de alta seguridad. Estos tipos de atacantes simplemente ven sus acciones como un medio por el cual las vulnerabilidades existentes de seguridad pueden estar expuestos.

  Los ataques de red se pueden clasificar en los siguientes cuatro tipos de ataques:

- Interior amenazas
- Amenazas externas:
  - amenazas no estructurados
  - amenazas Estructurado

Amenazas a la red se puede iniciar desde un número de diferentes fuentes, de ahí la razón por la cual los ataques de red se clasifican como ataques a la red externa y amenazas, o ataques de red internos y amenazas:

- *Las amenazas externas:* Las amenazas externas o ataques a la red se llevan a cabo por individuos sin la asistencia de los empleados internos o contratistas. Estos ataques suelen ser realizados por un individuo malicioso con experiencia, un grupo de personas con experiencia, una organización con experiencia maliciosos, o por atacantes sin experiencia ("script kiddies"). Las amenazas externas son generalmente se hace con un plan predefinido y las tecnologías (herramientas) o técnicas del atacante (s). Una de las principales características de las amenazas externas es que por lo general implica el análisis y recopilación de información. Por lo tanto, puede detectar un ataque externo mediante el examen firewall registros existentes. También puede instalar un sistema de detección de intrusiones para identificar rápidamente las amenazas externas.

Las amenazas externas pueden clasificarse en cualquiera de las amenazas estructuradas o no estructuradas:

- *Estructurado amenazas externas:* Estas amenazas provienen de un individuo malicioso, un grupo de individuo malicioso (s) o de una organización maliciosos. Estructurado amenazas suelen iniciarse a partir de los atacantes de red que tienen un pensamiento premeditado a los daños reales y las pérdidas que quieren causar. los motivos posibles de las amenazas externas estructuradas incluyen la codicia, la política, el terrorismo, el racismo y los pagos penales. Estos atacantes están altamente cualificados en el diseño de redes, los métodos sobre cómo evitar las medidas de seguridad, sistemas de detección de intrusiones (IDS), los procedimientos de acceso y herramientas de hacking. Ellos tienen los conocimientos necesarios para desarrollar nuevas técnicas de ataque a la red y la capacidad de modificar las herramientas de hacking para sus explotaciones. En algunos casos, el atacante podría ser asistido por una persona autorizada interior.
- *No estructurado amenazas externas:* Estas amenazas provienen de un atacante sin experiencia, por lo general de un script kiddie. Un script kiddie es la terminología utilizada para referirse a un atacante sin experiencia que utiliza herramientas de cracking o herramientas de secuencias de comandos disponibles en Internet, para realizar un ataque de red. “script kiddies” suelen ser mal calificados para crear las amenazas por su cuenta. “script kiddies” pueden ser considerados como individuos que buscan algún tipo aburrido de la fama al intentar accidente de sitios Web y otros objetivos públicos en Internet.

Los ataques externos también pueden ocurrir ya sea remota o local:

- *Remoto ataques externos:* Estos ataques son por lo general a los servicios que una organización ofrece al público. Las diversas formas que a distancia puede tener ataques externos se enumeran aquí:
  - Remoto ataques destinados a los servicios disponibles para los usuarios internos. Este ataque a distancia por lo general ocurre cuando no hay solución de firewall implementado para proteger a estos servicios internos.
  - Remoto ataques encaminados a la localización de los módems para acceder a la red corporativa.
  - De denegación de servicio (DoS) para colocar una carga de procesamiento en los servidores excepcionales en un intento de evitar que autoriza las solicitudes de usuario pueda dar servicio.
  - Guerra de marcación de la centralita de las empresas privadas (PBX).
  - Los intentos de la fuerza bruta contraseña autenticado sistemas.
- *Local ataques externos:* Estos ataques generalmente se originan en situaciones en las instalaciones de computación son compartidos, y el acceso a la red pueden ser obtenidos.

- *Las amenazas internas: los* ataques internos se originan en el interior de empleados descontentos o insatisfechos o contratistas. atacantes internos tienen alguna forma de acceso al sistema y por lo general tratan de ocultar su ataque como un proceso normal. Por ejemplo, los empleados descontentos internos tienen acceso local a algunos recursos de la red interna ya. También podría tener algunos derechos administrativos en la red. Uno de los mejores medios para proteger contra ataques internos es implementar un sistema de detección de intrusiones, y configurarlo para que busque los ataques externos e internos. Todas las formas de ataques deben ser registrados y los registros deben ser revisados y seguimiento.
  Respecto a los ataques de red, los componentes básicos que deben incluirse cuando la seguridad de su red de diseño son:

  - Red de prevención contra ataque.
  - Red de detección de ataques.
  - Red de aislamiento ataque.
  - Red de recuperación de ataque.

Amenazas: Interrupción, Intercepción, Modificación y Fabricación.

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Contra cualquiera de los tres elementos dichos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores [Olovsson, 1992) consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el "fabricado". En la figura 1.3 se muestran estos tipos de ataque de una forma gráfica.

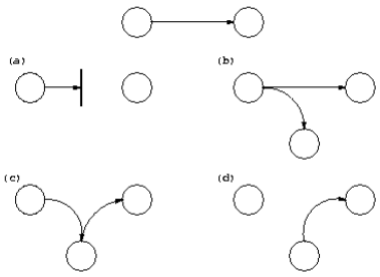


Figura 1.3: Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación **[Gallo, 2001].**

Ataques: DoS, Sniffing, Man in the middle, Spoofing, Pharming.

Ataque *man-in-the-middle o JANUS*

En criptografía, un **ataque *man-in-the-middle o JANUS*** (**MitM** o *intermediario*, en español) es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando éste se emplea sin autenticación.

Posibles subataques

El ataque MitM puede incluir algunos de los siguientes subataques:

- Intercepción de la comunicación (*eavesdropping*), incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos (*plaintext*) conocidos.
- Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- Ataques de sustitución.
- Ataques de repetición.
- Ataque por denegación de servicio (*denial of service*). El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes. La defensa en ese caso pasa por el envío periódico de mensajes de *status* autenticados.

MitM se emplea típicamente para referirse a manipulaciones activas de los mensajes, más que para denotar intercepción pasiva de la comunicación.

Defensas contra el ataque

La posibilidad de un ataque de intermediario sigue siendo un problema potencial de seguridad serio, incluso para muchos criptosistemas basados en clave pública. Existen varios tipos de defensa contra estos ataques MitM que emplean técnicas de autenticación basadas en:

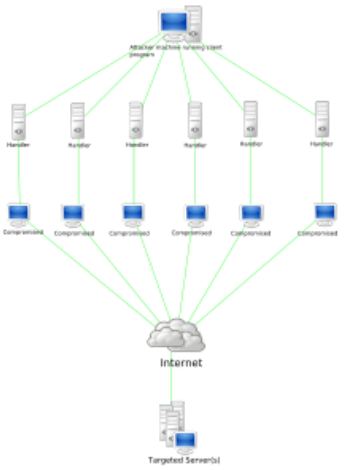
- Claves públicas
- Autenticación mutua fuerte
- Claves secretas (secretos con alta entropía)
- Passwords (secretos con baja entropía)
- Otros criterios, como el reconocimiento de voz u otras características biométricas

La integridad de las claves públicas debe asegurarse de alguna manera, pero éstas no exigen ser secretas, mientras que los passwords y las claves de secreto compartido tienen el requerimiento adicional de la confidencialidad. Las claves públicas pueden ser verificadas por una autoridad de certificación (CA), cuya clave pública sea distribuida a través de un canal seguro (por ejemplo, integrada en el navegador web o en la instalación del sistema operativo).

DoS- Ataque de denegación de servicio

En seguridad informática, un **ataque de denegación de servicio**, también llamado ataque **DoS** (de las siglas en inglés ***D**enial **o**f **S**ervice*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados Crackers para dejar fuera de servicio a servidores objetivo.



Una ampliación del ataque Dos es el llamado **ataque distribuido de denegación de servicio**, también llamado ataque **DDoS** (de las siglas en inglés***D**istributed **D**enial **o**f **S**ervice*) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS es a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.

En ocasiones, esta herramienta ha sido utilizada como un buen método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y afectar a los servicios que presta. Un administrador de redes puede así conocer la capacidad real de cada máquina

Sniffing -*analizador de paquetes*

En informática, un **analizador de paquetes** es un programa de captura de las tramas de una red de computadoras.

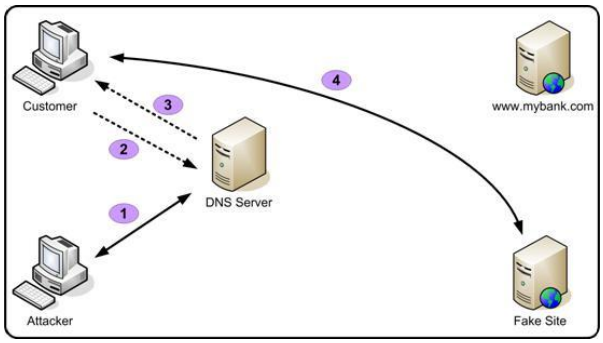
Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el analizador pone la tarjeta de red en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta; de esta manera se puede capturar (*sniff*, "olfatear") todo el tráfico que viaja por la red.

Los analizadores de paquetes tienen diversos usos, como monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.

Spoofing

Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

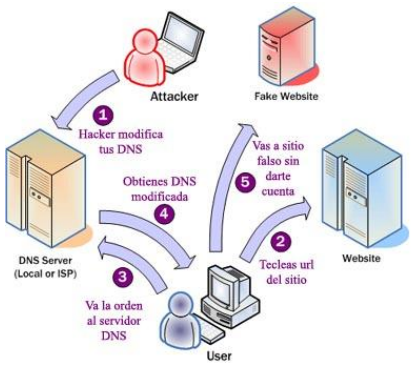
Se pueden clasificar los ataques de *spoofing*, en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.



- **Tipos de Spoofing**
  - IP Spoofing
  - ARP Spoofing
  - DNS Spoofing
  - Web Spoofing
  - Mail Spoofing

Pharming

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (*domain name*) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.



Método de funcionamiento del pharming

Todos los ordenadores conectados a internet tienen una dirección IP única, que consiste en 4 octetos (4 grupos de 8 dígitos binarios) de 0 a 255 separados por un punto (ej: 127.0.0.1). Estas direcciones IP son comparables a las direcciones postales de las casas, o al número de los teléfonos.

Debido a la dificultad que supondría para los usuarios tener que recordar esas direcciones IP, surgieron los Nombres de Dominio, que van asociados a las direcciones IP del mismo modo que los nombres de las personas van asociados a sus números de teléfono en una guía telefónica.

Los ataques mediante *pharming* pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados, o bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix.

La técnica de *pharming* se utiliza normalmente para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

- **Riesgos potenciales en los servicios de red:**

Seguridad en los dispositivos de red:

¿Qué se tiene que hacer?

- Enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- Describir procedimientos de seguridad y roles para interactuar con proveedores externos.

Seguridad física

- Designar el personal para actividades de instalación, desinstalación.
- Designar la persona para realizar actividades de mantenimiento.
- Designar la persona para realizar la conexión física.
- Definir controles de colocación y usos de la consola y los puertos de acceso.
- Definir procedimientos de recuperación ante eventualidades físicas.

Terminales

La seguridad en los terminales, es la seguridad que se consigue poniendo programas en los terminales como un antivirus, antimalware, antizombies etc…

Switch

Los puertos del switch pueden ser un punto de entrada a la red por parte de usuarios no autorizados. Para evitarlo, los switches ofrecen una función que se conoce como seguridad de puertos. La seguridad de puerto limita la cantidad de direcciones MAC válidas que se permiten por puerto. El puerto no reenvía paquetes con direcciones MAC de origen que se encuentran fuera del grupo de direcciones definidas.

Existen tres maneras de configurar la seguridad de puerto.

Estática

Las direcciones MAC se configuran manualmente con el comando de configuración de interfaz switchport port-security mac-address. Las direcciones MAC estáticas se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución.

Dinámica

Las direcciones MAC se aprenden de manera dinámica y se almacenan en la tabla de direcciones. Se puede controlar la cantidad de direcciones que se aprenden. La cantidad máxima predeterminada de direcciones MAC que se aprenden por puerto es una. Las direcciones que se aprenden se borran de la tabla si el puerto se desconecta o si el switch se reinicia.

Sin modificación

Similar a dinámica excepto que las direcciones también se guardan en la configuración en ejecución.

La seguridad del puerto se deshabilita de manera predeterminada. Si se habilita la seguridad del puerto una violación hace que el puerto se desconecte. Por ejemplo, si se habilita la seguridad de puerto dinámica y la cantidad máxima de direcciones MAC por puerto es uno, la primera dirección que se aprende se transforma en la dirección segura. Si otra estación de trabajo intenta acceder al puerto con una dirección MAC diferente se produce una infracción de seguridad.

Router

El mínimo es cambiar la contraseña que viene por defecto. Tendremos que generar una password fuerte que no sea fácilmente identificable por posibles atacantes. La segunda opción es tapar el agujero que puede suponer tener determinados puertos abiertos, cuestión que podemos evaluar con cualquier escaneado de puertos.

Por último una opción sencilla y que no evita ataques pero si curiosos merodeando por nuestro espectro es ocultar nuestra red WiFi. Además de las medidas de protección que hayamos tomado para proteger el acceso, mantener la red oculta a la detección automática nos evitará que más de un curioso se interese por nuestra red. Son medidas sencillas, que con un par de manuales de nuestro modelo de router podemos poner en práctica y tener un poco más de seguridad en nuestra red.

Seguridad de configuración estática

- Designar la(s) persona(s) que accede(n) al router vía consola o en forma remota.
- Designar la persona con privilegios de administración.
- Definir procedimientos para realizar cambios a la configuración.
- Definir políticas de password de usuario y administrador.
- Definir protocolos, procedimientos y redes para acceso remoto.
- Definir plan de recuperación que incluya responsabilidades individuales ante incidentes.
- Definir políticas de revisión de bitácoras.
- Definir procedimientos y limitaciones del monitoreo remoto (SNMP).
- Definir directrices para la detección de ataques directos.
- Definir políticas de administración e intercambio de información (Protocolos de ruteo, RADIUS, SNMP, TACAS+, NTP).
- Definir políticas de intercambio de llaves de encriptación.
- Seguridad de configuración dinámica
- Identificar los servicios de configuración dinámica del router, y las redes permitidas para acceder dichos servicios
- Identificar los protocolos de ruteo a utilizar, y sus esquemas de seguridad que proveen.

Seguridad de configuración dinámica

- Designar mecanismos y políticas de actualización del reloj (manual o por NTP).
- Identificar los algoritmos criptográficos autorizados para levantar VPN's.

WIFI

Si seleccionamos la opción wireless de nuestro router para configurarlo con seguridad nos aparecerán una serie de opciones comunes:

- **Esconder tu red**: Se trata de marcar una opción en la configuración para que cuando se realizan búsquedas de redes para conectarte no aparezca la tuya. En realidad, es como una protección contra curiosos. Previamente nosotros le hemos dado un nombre a nuestra red, generalmente en el apartado SSID donde nos aparecerá un nombre por defecto.
- **Deshabilitar el servidor DHCP**: Generalmente cuando queremos conectarnos a una red dejamos que sea el propio router el que nos asigne automáticamente una dirección IP. Si queremos que alguien no acceda a nuestra conexión podemos desactivar esta opción y asignar manualmente nosotros las direcciones IP a los equipos.

Filtrado de direcciones MAC: Esta es una de las medidas más efectivas a mi entender respecto a la seguridad inalámbrica. Como hemos visto anteriormente cada tarjeta de red tiene una dirección física única en el mundo para identificarse. Podemos indicarle al router que tarjetas de red se pueden

conectar, dejando operativas las de nuestros equipos cotidianos y denegando el resto. Con esto evitamos que aunque descubran nuestra contraseña o consigan acceder a nuestra red, el router no los reconozca como autorizados al no tener la dirección MAC del equipo extraño que quiere conectarse como autorizada en su lista

A parte de todas estas precauciones nos queda por contar que tipo de **contraseñas de seguridad y cifrad**o podemos ponerle a nuestra conexión para hacer que la información viaje lo más segura posible entre nuestro equipo y el modem router que nos conecta a internet. Como en todos los temas de seguridad es importante saber que **nada es infalible** y como todos hemos oído que se introducen en ordenadores de tal o cual organización, pues claro está que si lo intentan lo más probable es que consigan entrar en nuestra red.

Seguridad en los servicios de red por niveles:

El modelo OSI está pensado para que cada capa opere independiente de las demás.
Esto significa que una capa puede ser comprometida sin que las demás lo noten.

Ataque en la Capa Enlace de datos

Mitos de la capa de enlace de datos

- Las direcciones MAC no pueden ser falsificadas.
- Un switch no permite hacer sniffing.
- Las VLANs están completamente aisladas unas de otras.

Ataques basados en MAC y ARP:

CAM Table Overflow

- Los switchs guardan las asociaciones MACPuerto e información de VLAN a medida que las "aprenden" en un tabla llamada tabla CAM.
- La tabla CAM de un switch tiene un tamaño fijo y finito.
- Cuando la tabla CAM no tiene espacio para almacenar más asociaciones MAC-Puerto envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenado en la tabla CAM. (Actúa como un HUB para cualquier MAC que no haya aprendido)

• Se basa en el tamaño limitado de la tabla CAM.
• Para realizar el ataque sólo hace falta enviar gran número de tramas con direcciones MAC distintas (usualmente generadas al azar) a cualquier puerto del switch hasta que se llene la tabla CAM.
• Se desarrolló una herramienta para tal fin llamada macof.

Actualmente es parte del paquete Dsniff (GNU/Linux).

Address Resolution Protocol(ARP)

La solicitud ARP se coloca en una trama broadcast y se envía.
Todas las estaciones reciben la trama y examinan el pedido.
La estación mencionada en el pedido contesta y todas las demás estaciones procesan la misma.

Ataques que usan ARP Spoofing

Switch Port Stealing (Sniffing):

Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego re-enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario (Una especie de sniffig half-duplex).

Man in the Middle (Sniffing):

Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo (Inclusive en ambientes switcheados)

Secuestro (Hijacking):

Utilizando ARP Spoofing el atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación (previa deshabilitación del correspondiente dispositivo) y secuestrar la sesión.

Denial of service (DoS):

Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

Ataques basados en VLAN

Dinamic Trunk Protocol (DTP)

• Automatiza la configuración de los trunk 802.1Q/ISL.
• Sincroniza el modo de trunking en los extremos.
• Hace innecesaria la intervención administrativa en ambos extremos.

VLAN Hopping Attack

• Un equipo puede hacerse pasar como un switch con 802.1Q/ISL y DTP, o bien se puede emplear un switch.
• El equipo se vuelve miembro de todas las VLAN.
• Requiere que el puerto este configurado con trunking automático.

Double Tagged VLAN Hopping Attack

• Se envian una trama 802.1Q de la VLAN de la víctima dentro de otra trama 802.1Q de nuestra VLAN.

• Los switchs realizan un solo nivel de desencapsulado.
• Solo permite tráfico en una sola dirección.
• Sólo funciona si la VLAN nativa del trunk es la misma a la que pertenece el atacante.
• Funciona aunque el puerto del atacante tenga desactivado el trunking.

VLAN Trunking Protocol (VTP)

• Se lo emplea para distribuir configuraciones de VLAN a través de múltiples dispositivos.
• VTP se emplea únicamente en puertos trunk.
• VTP puede causar muchos inconvenientes.
• VTP emplea autenticación considere usar MD5.
• Si un atacante logra que su puerto se convierta en trunk, puede enviar mensajes VTP como si fuera un servidor VTP sin VLANs configuradas. Cuando los demás switches reciban el mensaje eliminarán todas sus VLANs.

¿Cómo protegerse?

Siempre utilizar una VLAN dedicada para los puertos trunk.

• Deshabilitar los puertos no utilizados y colocarlos en una VLAN no utilizada.
• No utilizar la VLAN 1 para nada.
• Colocar todos los puertos de los usuarios como non-trunking (Deshabilitar DTP)

Ataques basados en STP

• El atacante envía mensajes BPDU forzando recálculos STP.
• El atacante envía mensajes BPDU para convertirse en root.
• El atacante se convierte en root con lo cual puede ver tramas que no debería (esto permite ataques MiM, DoS, etc)
• Hace falta que el atacante esté conectado a dos switches simultáneamente.
El atacante envía mensajes BPDU anunciándose como bridge con prioridad 0.
• El atacante se vuelve root.
• Si se lo combina con MAC flooding este ataque puede permitir capturar más tramas.

¿Cómo protegerse?

- No deshabilitar STP (introducir un loop puede convertirse en una forma de ataque).
- Habilitar BPDU Guard: (Dentro del modo configuración global)

  Switch(config)# spanning-tree portfast bpduguard default

  (Dentro del modo configuración de interface del puerto a configurar)

  Switch(config-if)# spanning-tree bpduguard enable
  o
  Switch(config-if)# spanning-tree portfast

- Habilitar Root Guard:

  (Dentro del modo configuración de interface del puerto a configurar)
  Switch(config-if)# spanning-tree guard root

Ataque en la Capa Red (ip)
Sin medidas de seguridad, tanto las redes públicas como las privadas están expuestas a la observación y el acceso no autorizados. Los ataques internos pueden ser la consecuencia de una seguridad de intranet mínima o incluso inexistente. Los riesgos provenientes del exterior de la red privada se originan en las conexiones a Internet y a extranets. Los controles de acceso de usuarios basados en contraseñas no protegen por sí solos los datos transmitidos a través de una red.

Tipos comunes de ataques a redes
Si no se toman medidas de seguridad ni se aplican controles, los datos pueden ser objeto de un ataque. Algunos ataques son pasivos, en el sentido de que sólo se observa la información. Otros ataques son activos y se modifica la información con intención de dañar o destruir los datos o la propia red. Cuando no se tiene un plan de seguridad, las redes y los datos son vulnerables a todos los tipos de ataques siguientes.

Espionaje
En general, la mayoría de las comunicaciones por red tienen lugar en formato de texto simple (sin cifrar), lo que permite al atacante que haya logrado el acceso a las rutas de datos de una red observar e interpretar (leer) el tráfico. El espionaje de las comunicaciones por parte de un atacante se conoce como husmear. La capacidad de los espías para observar la red suele ser el mayor problema de seguridad que afrontan los administradores de las compañías. Sin unos servicios de cifrado eficaces basados en criptografía, mientras los datos atraviesan la red pueden ser observados por terceros.

Modificación de datos
Cuando un atacante ha leído los datos, a menudo el siguiente paso lógico consiste en modificarlos. Un atacante puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan. Incluso cuando no se requiera confidencialidad en todas las comunicaciones, no se desea que los mensajes se modifiquen en su camino. Por ejemplo, si intercambia solicitudes de compra, no desea que se modifique la información relativa a los artículos, los importes ni la facturación.

Suplantación de identidad (direcciones IP ficticias)
La mayoría de las redes y sistemas operativos utilizan la dirección IP para identificar un equipo como válido en una red. En algunos casos, es posible utilizar una dirección IP falsa. Esta práctica se conoce como suplantación. Un atacante podría utilizar programas especiales para construir paquetes IP que parezcan provenir de direcciones válidas dentro de la intranet de una organización.

Una vez obtenido el acceso a la red con una dirección IP válida, el atacante podrá modificar, desviar o eliminar datos. También podrá realizar ataques de otros tipos, como se describe en las secciones siguientes.

Ataques basados en contraseñas
Un procedimiento común en la mayoría de los sistemas operativos y planes de seguridad de redes es el control de acceso basado en contraseñas. El acceso tanto a un equipo como a los recursos de la red está determinado por un nombre de usuario y una contraseña.

Históricamente, muchas versiones de componentes de sistemas operativos no siempre protegían la información de identidad cuando ésta pasaba por la red para su validación. Ello podría permitir a un espía detectar un nombre de usuario y una contraseña válidos, y utilizarlos para lograr acceso a la red haciéndose pasar por un usuario autorizado.

Cuando un atacante encuentra una cuenta de usuario válida y la utiliza para el acceso, obtendrá los mismos derechos que el usuario real. Por ejemplo, si el usuario tiene derechos administrativos, el atacante puede crear cuentas adicionales para tener acceso posteriormente.

Una vez obtenido el acceso a una red con una cuenta válida, el atacante puede hacer lo siguiente:

- Obtener listas de nombres de usuarios y equipos válidos e información de la red.
- Modificar las configuraciones de los servidores y de la red, incluidos los controles de acceso y las tablas de enrutamiento.
- Modificar, desviar o eliminar datos.

Ataque de rechazo de servicio

A diferencia de un ataque basado en contraseñas, el ataque de rechazo de servicio impide el uso normal de un equipo o de una red por parte de los usuarios autorizados.

Una vez obtenido el acceso a una red, el atacante puede hacer lo siguiente:

- Distraer al personal de sistemas de información para que no detecte inmediatamente la intrusión. Esto da al atacante la oportunidad de llevar a cabo ataques adicionales.
- Enviar datos no válidos a aplicaciones o servicios de red para provocar su cierre o su funcionamiento de forma anormal.
- Generar tráfico masivamente hasta provocar el colapso de un equipo o de toda la red.
- Bloquear el tráfico, lo que hace perder el acceso a los recursos de la red por parte de los usuarios autorizados.

Ataque por usuario interpuesto

Como su nombre indica, un ataque por usuario interpuesto se produce cuando alguien situado entre dos usuarios que se están comunicando observa activamente, captura y controla la comunicación sin que los usuarios lo adviertan. Por ejemplo, un atacante puede negociar claves de cifrado con ambos usuarios. A continuación, cada usuario enviará datos cifrados al atacante, quien podrá descifrarlos. Cuando los equipos se comunican en niveles bajos de la capa de red, quizás no puedan determinar con qué equipos están intercambiando datos.

Ataque de clave comprometida

Una clave es un código o un número secreto necesario para cifrar, descifrar o validar información protegida. Averiguar una clave es un proceso difícil y que requiere grandes recursos por parte del atacante, pero no deja de ser posible. Cuando un atacante averigua una clave, ésta se denomina clave comprometida.

El atacante puede utilizar la clave comprometida para obtener acceso a una comunicación protegida sin que el remitente ni el receptor lo perciban. La clave comprometida permite al atacante descifrar o modificar los datos. El atacante también puede intentar utilizar la clave comprometida para calcular otras claves que podrían suponer el acceso a otras comunicaciones protegidas.

Ataque de husmeador

Un husmeador es una aplicación o dispositivo que puede leer, supervisar y capturar intercambios de datos y paquetes en la red. Si los paquetes no están cifrados, el husmeador proporciona una vista completa de los datos contenidos en el paquete. Incluso los paquetes encapsulados (enviados por un túnel) se pueden abrir y leer si no están cifrados.

El husmeador permite al atacante hacer lo siguiente:

- Analizar una red y lograr acceso a la información, y eventualmente hacer que la red deje de responder o que resulte dañada.
- Leer comunicaciones privadas.

Ataque en la Capa de aplicación

Los ataques en la capa de aplicación se dirigen a los servidores de aplicaciones e intentan provocar errores en su sistema operativo o en sus aplicaciones. De este modo el atacante puede llegar a eludir los controles de acceso normales. El atacante aprovecha esta situación para obtener el control de una aplicación, sistema o red, con lo que podrá hacer lo siguiente:

- Leer, agregar, eliminar o modificar datos o un sistema operativo.
- Introducir un virus que utilice los equipos y las aplicaciones de software para copiarse por toda la red.
- Introducir un programa husmeador que analice la red y obtenga información que pueda utilizarse para hacer que la red deje de responder o que resulte dañada.
- Cerrar aplicaciones de datos o sistemas operativos de forma anormal.
- Deshabilitar otros controles de seguridad para posibilitar futuros ataques

Ataque en la Capa Transporte (TCP-UDP)

SSL (Secure Socket Layer) es un protocolo criptográfico de la capa de aplicación
Proporciona autenticación, integridad y confidencialidad.
No proporciona "No repudio" Utiliza TCP Transparente para las capas superiores (aplicaciones).
Es el protocolo más utilizado en Internet para proporcionar servicios de seguridad
Utiliza criptografía simétrica y asimétrica desarrollado por Netscape hasta la versión 3.0
En el año 1996, en plena Guerra de Navegadores con Microsoft SSLv3.0 sirve de base al IETF para TLS Transport Layer Security, RFC 2246 (actualizado en la RFC 3546)

Problemas de seguridad

Restricción en la longitud de las claves utilizadas

Caracteristicas

- Fácil de utilizar e implementado en muchas aplicaciones
- Solo se aplica extremo a extremo
- Otras opciones implementadas por las aplicaciones
- Nivel de red seguro (IPSEC)

Distintas fases de trasporte

Fases en SSL

- Establecimiento de sesión
- Autenticación
- Negociación de los parámetros de cifrado que se utilizarán posteriormente
- Generar las claves
- Transferencia de Datos
- Proporcionando integridad y confidencialidad

Fase de Negociación (Handshake)

- Se negocian los algoritmos
- Algoritmo de cifrado simétrico y asimétrico
- Método de intercambio de claves

Funciones resumen

- Autenticación del servidor (obligatoria)
- Opcionalmente se autentica al cliente

ClientKeyExchange

- Envía cifrado el secreto premaestro calculado por el cliente
- Es la semilla de los algoritmos criptográficos que se utilizarán después
- Se cifra con la clave pública del servidor
- En este punto tenía lugar la debilidad de SSLv2, valores que deberían ser aleatorios no lo eran realmente

• Monitorización del tráfico en redes: Herramientas

El monitoreo es saber la disponibilidad de la maquina, tiempos de respuesta por medio del ping. Saber que servicios de red se encuentran habilitados, si están en funcionamiento o han dejado de funcionar y ver los paquetes que se envían y reciben con información. Se usan unas herramientas para realizar el monitoreo.

Los administradores de red pueden utilizar estas estadísticas para realizar tareas rutinarias de solución de problemas, como encontrar un servidor que no funciona o que está recibiendo un número desproporcionado de solicitudes de trabajo.

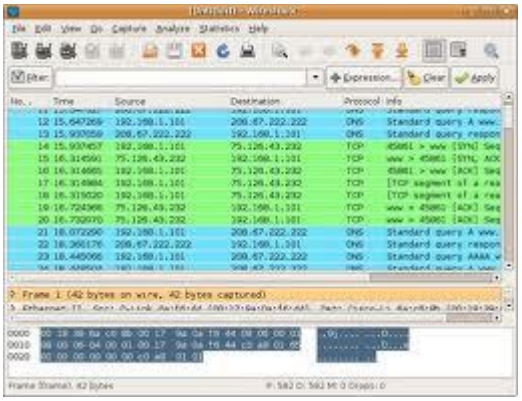
Estas herramientas muestran los tipos siguientes de información:

- La dirección de origen del equipo que envía una trama a la red. (Esta dirección es un número hexadecimal único (o en base 16) que identifica ese equipo en la red.)
- La dirección de destino del equipo que recibió la trama.
- Los protocolos utilizados para enviar la trama.
- Los datos o una parte del mensaje que se envía.

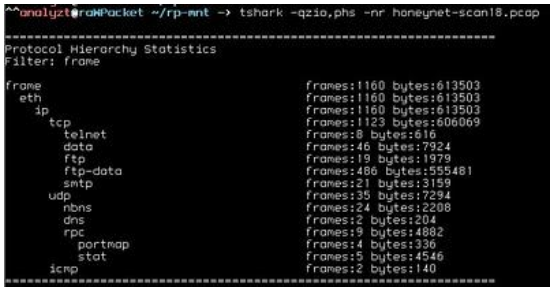
Monitorizacion en Linux

Etherape (etherape.sourceforge.net, *paquete etherape*): monitoriza gráficamente la actividad de toda la red (debe ejecutarse como *root*).

WireShark (antes **Ethereal**, *paquete wireshark*): monitoriza el tráfico de red (ejecutarlo como *root*).



TShark (*paquete tshark*): versión de WireShark para la línea de comandos. Por ejemplo, para capturar el tráfico entre nuestro equipo y otro haremos:

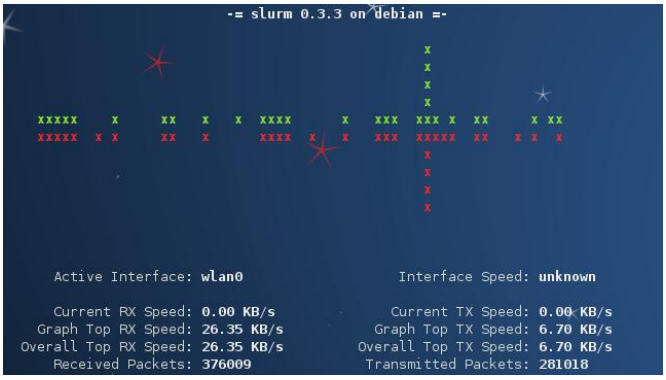


Aunque si sólo queremos conocer el tráfico de entrada y salida de nuestras interfaces de red en tiempo real sin capturar paquetes de datos disponemos de herramientas más sencillas, sin tener que utilizar un sniffer.

Slurm (*paquete slurm*)programa para la terminal que monitoriza gráficamente el tráfico de entrada y salida de cualquier interfaz de red en tiempo real. Utiliza el mismo código que el plugin para el panel de Xfce que monitoriza el tráfico de red .

Para ejecutar **Slurm**:

```
# slurm -i eth0
```



Monitorizacion en Windows

NetSpeedMonitor es una pequeña aplicación de monitoreo de redes que se instala en la barra de herramientas de nuestro sistema y nos permite saber en todo momento la velocidad de subida y de

bajada de datos de nuestras interfaces de red. También nos permite llevar un registro histórico de la cantidad de datos transmitida para ver las estadísticas diarias y mensuales. Además podemos ver una tabla con todas las conexiones TCP/UDP activas en tiempo real.

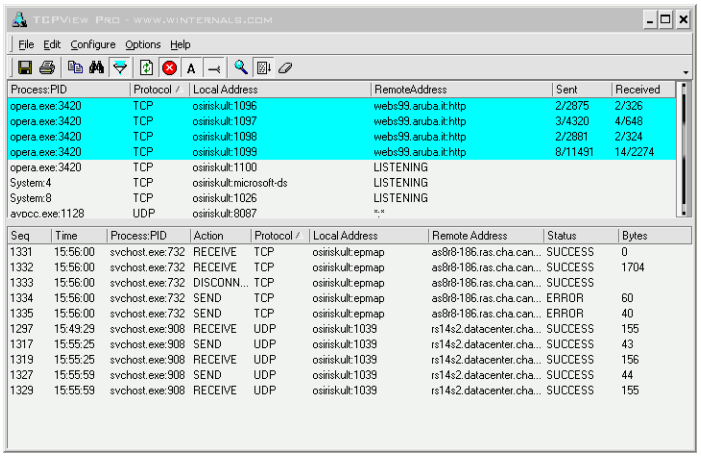
A diferencia de otras herramientas de monitoreo de redes, el **NetSpeedMonitor** no necesita instalar drivers adicionales para su funcionamiento.

La aplicación es compatible con **Windows XP, Windows Server 2003, Windows Vista y Windows 7**. Incluso con las versiones de 64bits.

Whireshark,Se trata de un analizador de protocolos que permite **realizar análisis y solucionar problemas en redes de comunicaciones**. Posee una interfaz gráfica que nos permitirá interpretar mejor la información que nos proporciona. Nos permite analizar todo el tráfico de una red ethernet, aunque también se puede utilizar en redes de otro tipo, estableciendo la configuración en modo promiscuo lo que le permite capturar todo el tráfico de la LAN.

Para sacarle todo el partido deberemos saber realizar filtros para la información recibida de forma que no nos veamos desbordados por la información que nos proporciona.

TCPView Pro es un programa muy útil a la hora de monitorear el trafico **TCP/IP** en cualquier sistema operativo Windows suministrándonos información vital sobre todas las conexiones activas así como sobre los programas o servicios que son responsables de esas conexiones y la cantidad de información enviada o recibida.



NetGong es un potente monitor de redes que vigila las conexiones activas y envía alarmas en caso de que fallen. Se configura fácilmente y es capaz de supervisar hasta 500 dispositivos de red o servicios.

En la pestaña Monitor, NetGong muestra las conexiones monitorizadas. Para añadir una, basta con hacer clic en Add y definir los parámetros: dirección del servidor, intervalos entre pings ICMP y tipos de alerta.

Los informes de NetGong se crean en formato HTML, listos para ser abiertos en cualquier navegador web.

- **Intentos de penetración:**

Sistemas de Detección de Intrusos (IDS).

El término **IDS** (*Sistema de detección de intrusiones*) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

- El grupo **N-IDS** (*Sistema de detección de intrusiones de red*), que garantiza la seguridad dentro de la red.
- El grupo **H-IDS** (*Sistema de detección de intrusiones en el host*), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.

El H-IDS se encuentra en un host particular. Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc.

.

El H-IDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).

Técnicas de Detección de Intrusos.

Técnicas de detección

El tráfico en la red (en todo caso, en Internet) generalmente está compuesto por datagramas de IP. Un N-IDS puede capturar paquetes mientras estos viajan a través de las conexiones físicas a las que está sujeto. Un N-IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y a las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones:

1. **Verificación de la lista de protocolos**: Algunas formas de intrusión, como "*Ping de la muerte*" y "*escaneo silencioso TCP*" utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada.
2. **Verificación de los protocolos de la capa de aplicación**: Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como "WinNuke", que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un N-IDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc.

Esta técnica es rápida (el N-IDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas falsas alarmas. Por ejemplo, al analizar protocolos, N-IDS puede diferenciar un "Back Orifice PING" (bajo peligro) de un "Back Orifice COMPROMISE" (alto peligro).

3. **Reconocimiento de ataques de "comparación de patrones"**: Esta técnica de reconocimiento de intrusión es el método más antiguo de análisis N-IDS y todavía es de uso frecuente.

   Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma específica. Por ejemplo, al buscar la cadena de caracteres "cgi-bin/phf", se muestra un intento de sacar provecho de un defecto del script CGI "phf". Este método también se utiliza como complemento de los filtros en direcciones IP, en destinatarios utilizados por conexiones y puertos de origen y/o destino. Este método de reconocimiento también se puede refinar si se combina con una sucesión o combinación de indicadores TCP.

   Esta táctica está difundida por los grupos N-IDS "Network Grep", que se basan en la captura de paquetes originales dentro de una conexión supervisada y en su posterior comparación al utilizar un analizador de "expresiones regulares". Éste intentará hacer coincidir las secuencias en la base de firmas byte por byte con el contenido del paquete capturado.

   La ventaja principal de esta técnica radica en la facilidad de actualización y también en la gran cantidad de firmas que se encuentran en la base N-IDS. Sin embargo, cantidad no siempre significa calidad. Por ejemplo, los 8 bytes “CE63D1D2 16E713CF”, cuando se colocan al inicio de una transferencia de datos UDP, indican un tráfico Back Orifice con una contraseña predeterminada. Aunque el 80% de las intrusiones utilicen la contraseña predeterminada, el 20% utilizarán contraseñas personalizadas y no serán necesariamente reconocidas por el N-IDS. Por ejemplo, si la contraseña se cambia a "evadir", la serie de bytes se convertirá en "8E42A52C 0666BC4A", lo que automáticamente la protegerá de que el N-IDS la capture. Además, la técnica inevitablemente conducirá a un gran número de falsas alarmas y falsos positivos.

   Existen otros métodos para detectar e informar sobre intrusiones, como el método Pattern Matching Stateful, y/o para controlar el tráfico peligroso o anormal en la red.

   En conclusión, un perfecto N-IDS es un sistema que utiliza las mejores partes de todas las técnicas mencionadas anteriormente.

Qué hacen los IDS

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers)**: Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).
- **Envío de una trampa SNMP a un hipervisor externo**: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.
- **Envío de un correo electrónico a uno o más usuarios**: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.
- **Registro del ataque**: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.
- **Almacenamiento de paquetes sospechosos**: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.
- **Apertura de una aplicación**: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).
- **Envío de un "*ResetKill*"**: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).
- **Notificación visual de una alerta**: Se muestra una alerta en una o más de las consolas de administración.

Tipos de IDS: (Host IDS, Net IDS).

Tipos de IDS

Existen dos tipos de sistemas de detección de intrusos:

1. **HIDS** (*HostIDS*): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.
2. **NIDS** (*NetworkIDS*): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

Software libre y comercial

Software Libre

Software Libre o no propietario son aquellos que están bajo una licencia libre y que su uso, modificación y distribución son permitidos a todos. Las principales licencias de software libre son GPL y LGPL. La primera, destinada a usuarios que puedan incorporarle modificaciones o que puedan agregar el software libre a un trabajo propio, el cual deberá ponerlo a disposición también con la misma licencia. La segunda, es más libre y destinada inclusive a software comercial.

Software Libre no implica necesariamente que es gratuito, este es un punto importante a considerar, muchos softwares libres pueden ser vendidos o incorporado a ellos la venta de consultoría o servicios anexos.

Ejemplos de Softwares Libres:

- Sistema Operacional Linux
- Lenguajes Java y PHP
- Base de datos MySQL
- Programa de oficina Open Office

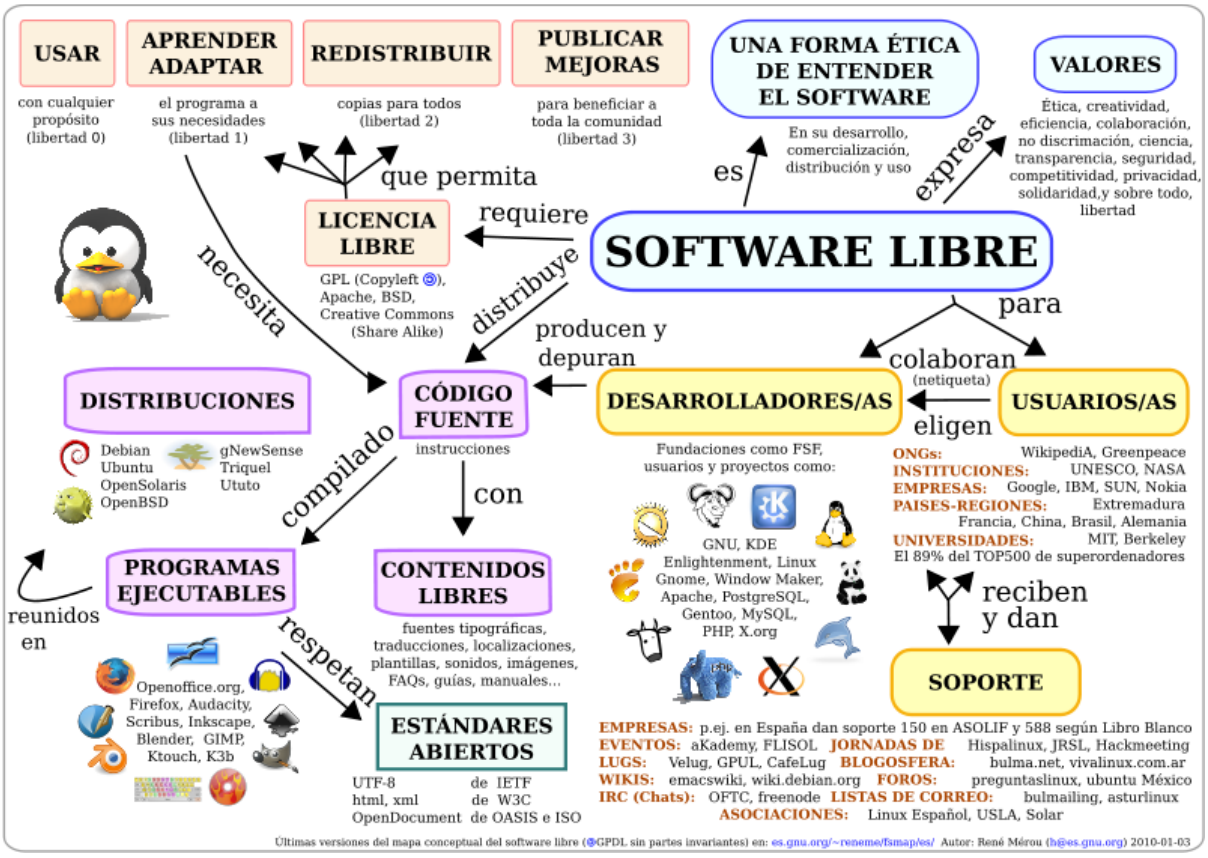
Software Comercial

El Software Comercial o propietario es aquel que tiene un dueño y su uso se permite mediante una licencia comercial y en la mayoría de las veces pagada. El Software Comercial no es diferente comercialmente de cualquier otro producto, sólo teniendo en cuenta que aún pagando por un software estarás recibiendo sólo la licencia o derecho de uso y no estarás comprando el software propiamente dicho.

Las empresas más importantes en el mercado de Software Comercial son: Microsoft, Adobe, Corel, Autodesk, Apple, entre otras.

Ejemplos de Softwares Comercial:

- Sistema operativo Windows
- Paquete de oficina Office (Word, Excel, Power Point)
- Aplicación para el tratamiento de imágenes Photoshop
- Suite para desarrollo web Dreamweaver, Flash y Fireworks
- Software para diseño gráfico vectorial Corel Draw


USAR
con cualquier propósito (libertad 0)
APRENDER ADAPTAR
el programa a sus necesidades (libertad 1)
REDISTRIBUIR
copias para todos (libertad 2)
PUBLICAR MEJORAS
para beneficiar a toda la comunidad (libertad 3)
que permita
UNA FORMA ÉTICA DE ENTENDER EL SOFTWARE
es
En su desarrollo, comercialización, distribución y uso
expresa
VALORES
Ética, creatividad, eficiencia, colaboración, no discriminación, ciencia, transparencia, seguridad, competitividad, privacidad, solidaridad,y sobre todo, libertad
LICENCIA LIBRE
GPL (Copyleft), Apache, BSD, Creative Commons (Share Alike)
requiere
SOFTWARE LIBRE
necesita
distribuye
para
producen y depuran
colaboran
(netiqueta)
eligen
DISTRIBUCIONES
Debian
Ubuntu
OpenSolaris
OpenBSD
gNewSense
Triquel
Ututo
CÓDIGO FUENTE
instrucciones
DESARROLLADORES/AS
USUARIOS/AS
Fundaciones como FSF, usuarios y proyectos como:
GNU, KDE
Enlightenment, Linux
Gnome, Window Maker,
Apache, PostgreSQL,
Gentoo, MySQL,
PHP, X.org
ONGs: WikipediA, Greenpeace
INSTITUCIONES: UNESCO, NASA
EMPRESAS: Google, IBM, SUN, Nokia
PAISES-REGIONES: Extremadura
Francia, China, Brasil, Alemania
UNIVERSIDADES: MIT, Berkeley
El 89% del TOP500 de superordenadores
compilado
con
reciben y dan
SOPORTE
reunidos en
PROGRAMAS EJECUTABLES
Openoffice.org,
Firefox, Audacity,
Scribus, Inkscape,
Blender, GIMP,
Ktouch, K3b
respetan
CONTENIDOS LIBRES
fuentes tipográficas, traducciones, localizaciones, plantillas, sonidos, imágenes, FAQs, guías, manuales...
ESTÁNDARES ABIERTOS
UTF-8 de IETF
html, xml de W3C
OpenDocument de OASIS e ISO
EMPRESAS: p.ej. en España dan soporte 150 en ASOLIF y 588 según Libro Blanco
EVENTOS: aKademy, FLISOL JORNADAS DE Hispalinux, JRSL, Hackmeeting
LUGS: Velug, GPUL, CafeLug BLOGOSFERA: bulma.net, vivalinux.com.ar
WIKIS: emacswiki, wiki.debian.org FOROS: preguntaslinux, ubuntu México
IRC (Chats): OFTC, freenode LISTAS DE CORREO: bulmailing, asturlinux
ASOCIACIONES: Linux Español, USLA, Solar
Últimas versiones del mapa conceptual del software libre (GPDL sin partes invariantes) en: es.gnu.org/~reneme/fsmap/es/ Autor: René Mérou (h@es.gnu.org) 2010-01-03

- ## Sistemas de seguridad en WLAN:

La revolución WiFi en todo el mundo significa poder conectarse en cualquier sitio dentro de una gran ciudad, donde suele haber redes sin cables en hogares y oficinas. Pero resulta triste comprobar que detrás de tanta generosidad no hay altruismo sino dificultades tecnológicas. Los propietarios de las conexiones no las cierran porque es demasiado complicado.

¿Abierto o cerrado?

Las redes WiFi pueden ser abiertas o cerradas. En una red abierta, cualquier ordenador cercano al punto de acceso puede conectarse a Internet a través de él, siempre que tenga una tarjeta WiFi incorporada, claro. En la red cerrada el ordenador detectará una red inalámbrica cercana disponible, pero para acceder habrá que introducir la contraseña. Es lo que suele ocurrir en los aeropuertos y algunos hoteles, donde la contraseña se obtiene previo pago.

Hasta hace poco se empleaba un sistema de cifrado llamado WEP (Wired Equivalent Privacy) para proteger las redes WiFi. Las transmisiones se cifran con una clave de 128 bits, y sólo los usuarios con contraseña pueden conectarse al punto de acceso. La mayoría de las tarjetas y puntos de acceso WiFi son compatibles con WEP, pero este sistema está desconectado por defecto. Los usuarios por lo general no se molestan en activarlo, y la red queda abierta. Si el vecino de al lado utiliza de vez en cuando la conexión de Internet quizá no sea demasiado grave, pero cuando accede a información confidencial de la empresa o a fotos comprometidas de las vacaciones la cosa es más seria.

Hoy se utiliza un sistema de seguridad llamado WPA, que son las siglas de WiFi Protected Access. Este sistema está incluido en Windows XP con Service Pack 1, es más seguro que WEP y mucho más fácil de utilizar.

REDES CERRADAS

La mayoría de los puntos de acceso o *routers* sin cable funcionan nada más conectarlos, o vienen configurados por el operador. Pero si se quiere modificar algo, como la seguridad, conviene conocer algunos de los parámetros de la conexión:

- **El identificador SSID**: es el nombre de la red WiFi que crea el punto de acceso. Por defecto suele ser el nombre del fabricante ("3Com" o "Linksys"), pero se puede cambiar y poner "PerezWiFi", por ejemplo.
- **El canal**: por lo general se usa el canal 6, pero si el vecino también tiene un punto de acceso en este canal habrá que cambiarlo para evitar interferencias. Puede ser un número entre 1 y 11.
- **La clave WEP**: si se utiliza WEP para cerrar la red WiFi, hay que indicar la contraseña que tendrá que introducirse en los ordenadores que se quieran conectar.

- **La clave compartida WPA**: Como en el caso anterior, si se emplea seguridad WPA hay que seleccionar una clave de acceso para poder conectarse a la red WiFi.
- **Cifrado de 128 bits**: En WEP y WPA las comunicaciones se transmiten cifradas para protegerlas. Esto quiere decir que los números y letras se cambian por otros mediante un factor. Sólo con la clave adecuada se puede recuperar la información. Cuanto más grande sea el factor de cifrado (más bits), tanto más difícil resulta romper la clave.

La seguridad con WEP tiene algunos defectos. Las claves puede que no funcionen bien si se utilizan tarjetas y puntos de acceso de distintos fabricantes, por ejemplo. Con WPA esto queda solucionado con una clave o *secreto compartido* que puede tener entre 8 y 63 caracteres de largo.

Lo que hace a WPA más seguro es que la clave se cambia automáticamente cada cierto tiempo, y se actualiza en todos los equipos conectados. Hay un sistema que se encarga de distribuir las nuevas claves de forma segura llamado TKIP.

SEGURIDAD Y FIABILIDAD

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables a los hackers), sin proteger la información que por ellas circulan.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado, debido a las grandes vulnerabilidades que presenta, ya que cualquier cracker puede conseguir sacar la clave.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.

- El protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

  Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

• Recomendaciones de seguridad en WLAN:

Recomendaciones de seguridad en WLAN.

Para finalizar esta serie de notas sobre la seguridad para redes WIFI, entregamos algunos consejos finales para mejorar la seguridad.

- Instale el router en el ambiente más alejado de la calle y las ventanas. Muchos routers permiten controlar la intensidad de la señal, por esto, disminuya la intensidad para restringir la propagación fuera del edificio.

- Cambie la contraseña por default del router inalambrico: en general, el nombre de usuario es admin y la contraseña también es admin.

- Cambie el SSID por default del router inalambrico y deshabilite el broadcast del SSID. Si es posible, no hay que permitir acceder a la red local a través de la red inalámbrica sino solamente a través de la red cableada conectada a uno de los puertos LAN del router.

- Utilice WPA, en caso de que no estar disponible utilice WEP con una contraseña de 128 bits, si es posible.

- Instale actualizaciones de firmware cuando esten disponibles por el fabricante.

- Desconecte el router o deshabilite la red inalámbrica cuando no la utilice.

- Tenga siempre en mente la seguridad de todo el sistema instalando un firewall, actualizando el antivirus, el sistema operativo y los programas.

- Establecer y hacer cumplir las políticas de fuerte autenticación para los dispositivos que intentan acceder a redes corporativas.
- Establecer el uso obligatorio de una VPN corporativa y el cifrado cuando se hacen conexiones e intercambio de datos. Mejor aún, instalar computadoras y otros dispositivos móviles para que se conecten automáticamente a los datos cifrados de la VPN, de esta forma se pueden determinar sí el dispositivo no ha sido extraviado o robado.
- Cerciorarse de que todos los dispositivos y aplicaciones de software están configurados correctamente y tienen los últimos parches.

- Asegurarse que las políticas de seguridad corporativa prohíban a las personas la transferencia de datos sensibles a dispositivos móviles o equipos no autorizados.

  Proporcionar a los trabajadores tarjetas de acceso a la banda ancha que requieren un plan de servicio, para que los empleados no tengan que usar los puntos de acceso públicos para conexiones inalámbricas.

- **Bibliografía:**

http://haddensecurity.wordpress.com/2010/08/19/entendiendo-los-ataques-de-red/
http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf
http://es.wikipedia.org
http://es.kioskea.net/contents/detection/ids.php3
http://www.canal-ayuda.org/a-seguridad/tipataques.htm
http://ma1.eii.us.es/Material/Cripto_ii_Introduccion.pdf
http://www.malwareint.com/docs/attack-es.pdf
http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/Criptografia_Simetrica
http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/Criptografia_Asimetrica
http://www.inteco.es/extfrontinteco/img/File/intecocert/dnie/pdf/presentacion_dnie.pdf
http://www.dnielectronico.eu/
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-boot-sec.html
http://www.acrosoft.net/productos/hid/accesologico.shtml
http://technet.microsoft.com/es-es/library/cc758166(WS.10).aspx
http://cert.inteco.es/Proteccion/Actualizaciones_SW/
http://arco.esi.uclm.es/~david.villa/seguridad/modulo-B-I.2x4.pdf
http://www.nachox.com/2008/12/23/tipos-de-antivirus/
http://usuarios.multimania.es/cursosimm/capitulo13.htm
http://www.zonavirus.com/antivirus-on-line/
http://www.anexom.es/tecnologia/mi-conexion/configura-tu-router-la-seguridad-inalambrica-i/
http://www.tecnologiapyme.com/hardware/blindar-la-seguridad-en-el-acceso-al-router
http://www.routerwifi.com.ar/mantener-seguridad-router.php
http://technet.microsoft.com/es-es/library/bb821258.aspx
http://technet.microsoft.com/es-es/library/cc783463%28WS.10%29.aspx