Introducción.

Uno de los temas que es inevitable comentar en la actualidad al hablar de Internet y de la posibilidad de realizar negocios en la red, es la seguridad. El conocimiento popular indica que la Internet es "insegura", pero se ha dado poca o ninguna explicación acerca del porqué.

Con el fin de ofrecerle más información al respecto le presentamos dos artículos sobre el tema, realizados por las empresas Microsoft y Netscape.

En estos últimos 4 años el comercio en internet a puesto contra la pared a las leyes y los sistemas de seguridad, por esto , cada día se diseñan sistemas mas seguros. Pero es la naturaleza de la red , un Híbrido, que no permite que las transacciones, que se basan en el concepto básico de la confianza , puedan ser seguras.

En este trabajo tratamos algunos aspectos de la seguridad en internet , particularmente con el mas con el mas controversial de ellos, el comercio electrónico. ¿Es seguro comprar con su tarjeta de cerdito a través del internet? Responderemos a estas preguntas en las siguientes paginas, pero lo que si es cierto , es que la internet esta lejos de ser segura para cualquier cliente indefenso.

¿Es seguro el comercio por internet?

Uno de los temas que es inevitable comentar en la actualidad al hablar de Internet, y de la posibilidad de realizar negocios en la red, es el tema de la seguridad. El conocimiento popular indica que la Internet es "insegura", pero se ha dado poca o ninguna explicación de porqué.

Primero que todo, es importante explicar cuáles son los aspectos de seguridad que es necesario considerar cuando se ingresa al mundo "virtual" de la Internet.

Hoy, cuando una persona desea comprar algo, supongamos un libro, se dirige a la librería, selecciona el volumen que va a adquirir, y lo presenta al empleado de la librería junto con su tarjeta de crédito. El empleado de la librería llama a la compañía que emite la tarjeta de crédito y solicita la autorización de la compra. En caso extremo, puede solicitar al cliente una identificación con fotografía.

Si todo esta en orden, la compra es permitida, se otorga un número de autorización y listo. La persona vuelve a su casa con el libro bajo el brazo y, al final del mes, recibe el estado de cuenta con un cargo correspondiente.

Un hecho comúnmente olvidado por los detractores de Internet es que el uso de una tarjeta de crédito en una compra "tradicional" implica en ocasiones un riesgo, ya que el empleado de la librería, en este caso, el restaurante u otro comercio en otros casos, puede anotar nuestro nombre, número de tarjeta de crédito y fecha de expiración de la misma, copiándolo del "voucher", una vez que hemos abandonado el establecimiento.

Examinemos ahora que implica la realización de la misma operación, pero a través de Internet:

- La persona que desea comprar el libro se dirige a una librería "virtual" en Internet. Se conecta al sitio Web de la misma y examina la lista de títulos disponibles hasta encontrar la descripción de la que desea.

Problema 1:¿Cómo puede el comprador en potencia estar seguro de que el sitio Web que aparece en su pantalla es realmente el de la empresa que busca, y no un sitio Web que está "suplantando" al verdadero? En la vida diaria, este problema no existe porque el comprador potencial se dirige a la librería que está ubicada en un edificio específico y entra en ella. No hay duda entonces en dónde ésta el comprador.

- Una vez seleccionado el título, ordena la compra y al mismo tiempo envía a través de Internet su número de tarjeta de crédito y la fecha de expiración.

  Problema 2: ¿Cómo puede la librería estar segura de que la persona es verdaderamente quien dice ser y no alguien que se está haciendo pasar por una persona honrada a través de la Internet? En la vida diaria, esta verificación se realiza al comparar la firma que el comprador escribe en el "voucher" con la firma en el dorso en la tarjeta de crédito.

Problema 3: ¿Cómo pude el comprador enviar su información a través de Internet sin correr el riesgo de que alguien esté "interviniendo" las líneas de comunicación y registre su nombre, número de tarjeta de crédito y fecha de expiración, para usarlos más tarde a fin de cometer fraude?

- La orden es recibida por la librería, la cual debe solicitar a la compañía que emite la tarjeta de crédito la autorización para la compra. Si todo está en orden, la compra es permitida, se otorga un número de autorización y listo.
- El libro es enviado por correo o mensajería al comprador.

En la actualidad, solo el problema 3 tiene algún tipo de solución más o menos extendida en Internet, y aún en estos casos, limitada.

El problema 2 ha recibido una solución parcial, aplicable sólo en el caso de sitios Web que cobran al usuario por el acceso al contenido, es decir, a la información disponible en el mismo.

Esta solución radica en solicitar al usuario que seleccione una clave o password al momento de registrarse por primera vez.

El inconveniente de esta opción radica en que si el usuario desea utilizar los servicios de diferentes sitios Web necesita recordar un password diferente para cada uno.

Este mismo problema tiene una solución práctica: a partir del momento en el que el comerciante recibe el pedido electrónico hasta que entrega el libro en el domicilio del cliente habrá tiempo suficiente para descubrir el fraude, si lo hubiese.

Por lo que se refiere al problema 3, la solución en uso actualmente radica en codificar la información transmitida por el usuario al sitio Web del comerciante. Este proceso, que utiliza un estándar de codificación de información, conocido como SSL, impide a cualquier persona ajena al cliente y al comerciante conocer los datos transmitidos.

SSL es un sistema de codificación basado en un sistema estándar conocido como DES (Data Encryption System), desarrollado por el gobierno de Estados Unidos para permitir la comunicación segura entre organismos gubernamentales, y por lo tanto sujeto a grandes restricciones de exportación.

Esto soluciona el problema pero deja dos puntos descubiertos. El comerciante de todas maneras obtiene y almacena en su computadora el nombre, número de tarjeta de crédito y fecha de expiración del cliente.

Esto significa que las compañías que fabrican productos para Internet como visores y servidores Web que utilizan esta tecnología, no tienen autorización para venderlos fuera de Estados Unidos y Canadá, a menos que se utilice una versión "limitada" de dicho esquema. Es decir, una versión cuyo código es más fácil de "romper" si se cuenta con el poder de cómputo y conocimiento matemático adecuados.

Certificados de Identidad.

Microsoft Corp., Trabajando en conjunto con una serie de compañías interesadas a dar una solución a este caso, como es el de Visa y MasterCard, ha propuesto varias iniciativas a través del Microsoft Internet Security Framework (MSIF).

Este sistema contiene una serie de estándares que permitirán a las compañías desarrolladoras de software dar respuesta en sus productos a los problemas mencionados.

En este artículo sólo mencionaremos aquellos componentes de MSIF más relevantes.

Primero, con miras a solucionar los problemas 1 y 2, MSIF propone la utilización de "certificados" de identidad electrónicos.

Esto quiere decir que cada usuario y cada sitio Web en Internet tendrán un identificador electrónico único, extremadamente difícil de copiar, que les permitirá garantizar su identidad en la red.

Los certificados son expedidos por una compañía que actúa como autoridad de certificación de identidad llamada Verisign.

El certificado es proporcionado por la compañía y registrado por el visor de Internet por el usuario.

A partir de ese momento, cuando el cliente se conecte a un sitio Web, este le pedirá el certificado, verificará su autenticidad y permitirá entonces el acceso a los servicios disponibles.

Por su parte, el visor del cliente solicitará al sitio Web su propio certificado y lo verificará, para dar garantía al usuario de que efectivamente se trata del sito Web que buscaba. El componente de MISF que da solución al problema 3, aún está en proceso de definición en comité de estándares, en el que además de Microsoft están incluido Visa, Master Card y otras compañías desarrolladoras de tecnología.

El estándar es conocido como "Secure Electronic Transaction", el cual permite la codificación de un número ilimitado de datos, como el número de tarjeta de crédito y fecha de expiración para su transmisión al comerciante.

El comerciante recibe los datos y los transmite electrónicamente a al compañía que expide la tarjeta de crédito o que actúa como intermediaria entre el comerciante y el banco o compañía de tarjetas de crédito y, si todo está bien, obtiene la autorización de la operación.

Este esquema presenta dos grandes ventajas. Por una parte, el comerciante retransmite los datos codificados. Si todo está en orden, el comerciante recibirá la autorización de la operación y podrá entonces expedir los bienes, pero nunca conocerá el número de tarjeta de crédito ni fecha de expiración de la misma. Tan sólo sabrá que la operación fue autorizada y los datos necesarios para entregar el bien o servicio al cliente.

SET sólo codifica la información indispensable, a diferencia de SSL que codifica toda la información transmitida, cualquier cosa, sea texto o gráficos.

No sólo se usa para operaciones comerciales como el caso que aquí hemos descrito, sino para prácticamente cualquier aplicación que transmita, desde una letra hasta planos y planes completos para una operación terrorista, lo cual es precisamente la razón por la que su exportación está restringida en Estados Unidos.

Siendo SET algo tan específico, sólo para operaciones de tarjetas de crédito, es más probable el que el gobierno estadounidense autorice la exportación de productos con esta funcionalidad, sin restricciones.

Tópicos relacionados

1 − SSL.

2 − Firewalls.

3 − Proxy.

4 − Intranet

5 −−Encriptación

SSL

¿Qué es un servidor SSL?

Un servidor SSL permite la transmisión de datos confidenciales sin riesgo de que un intermediario obtenga la información.

¿Cómo puedo usarlo?

Es muy fácil. Escriba **https://**... en lugar **de http://**...

¿Porqué me hace falta un certificado?

Si no tiene su propio certificado instalado, Netscape y otros navegadores darán una advertencia al usuario.

¿Cómo puedo obtener un certificado?

Es imprescindible obtener el certificado de una autoridad reconocida, o no servirá para nada. Recomendamos a Thawte, porque sus tarifas son razonables ($125 USD al año) y sus certificados están reconocidos por Netscape 3, MS Explorer 3.01 y versiones posteriores.

Hay que dar los siguientes pasos:

- Nosotros le hacemos una petición de certificado ('Certificate Signing Request') que es enviado de forma electrónica e inmediata al cuerpo de emisión de certificados. En este momento tiene que abonar la cantidad del certificado.
- Usted tiene que mandar las pruebas de su identidad y el resto de la documentación al cuerpo de emisión de certificados.
- Cuando le aprueben su certificado le instalamos el certificado en su dominio

Para un certificado de Thawte, hace falta la siguiente documentación:

- Nota del registro de la Sociedad. (Obtenida del Registro Mercantil).
- Fotocopia compulsada del DNI. de los representantes legales de la Sociedad. (Administradores)
- Fotocopia del alta y último pago del Impuesto de Actividades Económicas (I.A.E.)
- Una carta autorizada solicitando este certificado de Thawte y además mencionando la petición del nombre (del dominio) que desea ser certificada.
- Esta solicitud estará firmada por la persona con poderes para ello.

En muchos casos será por ejemplo el director o el gerente de una empresa u organización.

Para poder crear una petición de un certificado ('Certificate Signing Request'), necesitamos los siguientes

datos:

- El nombre del dominio para lo cual desea el certificado. Por ejemplo **www.su−dominio.com**.
- Los detalles de la persona que va a firmar la carta autorizada: Nombre completo, nombramiento (del firmante) y número de teléfono.
- Dirección, número de fax, y email de la empresa
-

Firewall

Los Firewalls son un tipo de seguridad muy efectiva en redes. Intenta prevenir los ataques de usuarios externos a la red interna. Tiene múltiples propósitos:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques
- Restringir los permisos de los usuarios a puntos cuidadosamente controlados.

Un Firewall es a menudo instalado en el punto donde la red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del Firewall, así puede determinar si dicho tráfico es aceptable, de acuerdo a sus políticas de seguridad. Lógicamente un Firewall es un separador, un analizador, un limitador. La implementación física varia de acuerdo al lugar. A menudo, un Firewall es un conjunto de componentes de hardware − un router, un host, una combinación de routers, computadoras y redes con software apropiado.

Rara vez es un simple objeto físico. Usualmente esta compuesto por múltiples partes y alguna de esas partes puede realizar otras tareas. La conexión de Internet también forman parte del Firewall.

Un Firewall es vulnerable, él no protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna.

Un Firewall es la forma más efectiva de conectar una red a Internet y proteger su red.
Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad.

Las dos principales aproximaciones usadas para construir Firewalls hoy son:

- Filtrado de paquetes
- Servicio Proxy

Filtrado de paquetes:

El sistema de filtrado de paquetes rutea paquetes entre host internos y externos, pero de manera selectiva. Permite bloquear cierto tipo de paquetes de acuerdo con la política de seguridad de la red. El tipo de ruteo usado para filtra paquetes en un Firewall es conocido como "screening router".

Se puede selectivamente rutear paquetes desde o hacia su sitio:

- Bloquear todas las conexiones que entran desde sistemas externos, excepto las conexiones SMTP (solo recibirá mails)
- Bloquear todas las conecciones que provienen de un determinado lugar que se considera peligroso
- Permitir servicio de Mail y FTP, pero bloqueando servicios peligrosos como TFTP, RPC, servicios "r" (rlogin, rsh, etc), etc.

Para entender como se filtra un paquete, se necesita conocer la diferencia entre ruteo ordinario y "screening router".

Un ruteo ordinario simplemente mira la dirección destino de cada paquete y elige el mejor camino que el conoce hacia la dirección destino. La decisión sobre como atender el paquete se basa solamente en el destino del paquete.

En "screening router", mira el paquete más detalladamente. Además de determinar si el paquete puede ser ruteado o no a la dirección destino, determina si debe o no debe ser ruteado de acuerdo a la política de seguridad. La comunicación entre la red interna y externa tiene una enorme responsabilidad. Realizar el ruteo y la decisión de rutear es la única protección al sistema. Si la seguridad falla, la red interna estará expuesta. Un "screening router" puede permitir o denegar un servicio, pero no puede proteger operaciones individuales dentro del servicio.

Casi todos los dispositivos actuales de filtro de paquetes (enrutadores de selección o compuertas de filtro de paquetes) operan de la siguiente forma:

- El criterio de filtro de paquete debe almacenarse para los puertos del dispositivo para filtro de paquetes. El criterio de filtro de paquetes se conoce como reglas de filtro de paquetes.
- Cuando un paquete llega al puerto, los encabezados de los paquetes se analizan. La mayoría de los filtros los campos sólo en los encabezados IP, TCP o UDP.
- Las reglas del filtro de paquete se almacenan en un órden específico. Cada regla se aplica al paquete en el mismo orden en que la regla del filtro de paquetes se almacenó.
- Si una regla bloque la transmisión o recepción del paquete, el paquete no se acepta.
- Si una regla permite la transmisión o recepción de un paquete, el paquete sigue su camino.
- Si un paquete no satisface ninguna regla, el bloqueado. Es decir aquello que no esté expresamente permitido, se prohibe

En las reglas 4 y 5, deberá observar que es importante colocar las reglas en orden correcto. Un error común al configurar las reglas del filtro de paquetes es hacerlo en desorden. Si dichas reglas se colocan en un orden equivocado, podría terminar denegando servicios válidos, mientras que permitiría los servicios que deseaba denegar.

Servidor Proxy

Proxy es un sistema intermediario entre hosts internos de una red y los hosts de Internet de forma tal que reciba las requisiciones de unos y se las pase a los otros previa verificación de accesos y privilegios.

Este sistema puede correr en hosts "dual−homed" o hosts "bastion" los cuales serán llamados Servidores Proxy. La siguiente figura ilustra un servidor Proxy corriendo en un host "dual−homed".

Los sistemas Proxy son efectivos solo si se utilizan junto a métodos de restricción de tráfico IP entre clientes y servidores reales. De este modo, un cliente no podrá "bypasear" el servidor Proxy para comunicarse con un servidor real utilizando este protocolo.

Funcionamiento:

El programa cliente del usuario se comunica con el servidor Proxy enviando pedido de conexión con un servidor real.

El servidor Proxy evalúa esta requisición y decide si se permitirá la conexión.

Si el servidor Proxy permite la conexión, envía al servidor real la solicitud recibida desde el cliente. De este modo, un servidor Proxy se ve como "Servidor" cuando acepta pedidos de clientes y como "cliente" cuando envía solicitudes a un servidor real.

Una vez que establecida la comunicación entre un cliente y un servidor real, el servidor Proxy actúa como un retransmisor pasando comandos y respuestas de un lado a otro.

Un punto importante a tener en cuenta en este tipo de conexión es que es totalmente transparente. Un usuario nunca se entera de que existe un "intermediario" en la conexión que ha establecido. La Figura 2 ilustra este esquema de comunicación.

La comunicación entre el programa cliente y el servidor Proxy puede realizarse de dos formas distintas:

- *Custom Client Software*: El cliente debe saber como opera el servidor Proxy, como contactarlo, como pasar la información al servidor real, etc. Se trata de un software cliente standard que ha sido modificado para que cumpla ciertos requerimientos.
- *Custom User Procedures*. El usuario utiliza un cliente standard para conectarse con un servidor Proxy y usa diferentes procedimientos (comandos del servidor Proxy) para pasar información acerca del servidor real al cual quiere conectarse. El servidor Proxy realiza la conexión con el servidor real.

◊ Intranet

Aquellas redes que aprovechan el uso de la red Internet para fines privados forman lo que se conoce como intranet. La gran diferencia entre Internet e intranet es simplemente la forma de utilizar la red de redes. Internet es para todo público, mientras que intranet es sólo para los usuarios autorizados.

Los usuarios de la red Internet tienen acceso a la información almacenada en múltiples servidores conectados entre sí, mientras que los usuarios de intranet sólo tienen acceso a aquella información a la cual están previamente autorizados. La clave del intranet está en que todo el que desee tener acceso a la información de un servidor determinado tiene que tener la clave de acceso a él. De lo contrario, el acceso a dicha información le será denegado.

.

Descripción general

Una red de tipo Intranet es aquella en la cual se utilizan las herramientas del Internet (dígase los protocolos y las ayudas correspondientes) o la red misma, para fines particulares de una empresa.

Así como el Internet permite enlazar equipos físicamente muy distantes, el intranet permite enlazar personas físicamente alejadas entre sí, pero agrupadas en "islas" con sus propios servidores, sus propios equipos de cómputo, etc. La clave está entonces en que utilizan la tecnología de Internet, pero que operan en forma totalmente aislada: el servidor de cada una de las "islas" no puede ser accesado por personas ajenas a la empresa, o sea, por usuarios no autorizados.

Una red intranet puede o no tener acceso a Internet. Esto significa que dependiendo de su configuración, los usuarios de la misma pueden comunicarse sólo entre si o bien, pueden comunicarse con sus colegas y a la vez con el exterior.

Considerando que una red consta de un conjunto de equipos de cómputo conectados a un servidor, si una empresa tiene varios servidores ubicados en lugares geográficamente distantes, la conexión entre dichos servidores puede ser la clave para la comunicación entre los equipos conectados a cada uno de ellos. Dicha conexión puede ser:

- privada (o sea que conste de cables físicamente instalados por la organización a la que pertenecen los servidores).
- pública (en cuyo caso se aproveche la red instalada de las compañías de teléfonos).

En el primer caso, el costo de instalación puede ser sumamente elevado, mientras que en el segundo, dicho costo puede reducirse notablemente. La clave en el segundo caso consiste en utilizar un programa especial de acceso a los servidores que no permita la consulta de información por personas ajenas a la empresa, o sea, por usuarios externos. Dicho programa es el que impide el paso o el acceso en base a tablas de "personas autorizadas": Todo el que no esté previamente registrado en el servidor no puede accesar la información en él almacenada.

· **Ventajas del intranet**

A pesar de lo que pudiera creerse, la definición de un intranet no es exclusiva de empresas grandes. Puede resultar de suma utilidad para cualquier empresa con necesidades de comunicaciones entre computadoras físicamente distantes.

Una de las ventajas del intranet es el hecho de manejar la información de la empresa como si se tratase de páginas electrónicas del Web. La difusión de información se hace entonces a través de la red y ya no por medio de circulares u otro tipo de documentos. De esta manera, toda la información importante para los empleados de la empresa (por ejemplo, políticas de personal, directorio interno, cartera de clientes, control de inventarios, etc.) es manejada a través del intranet.

Las principales ventajas del manejo electrónico de información son las siguientes:

- Actualización . todo el personal tiene acceso a la información en el instante en que esta es actualizada. Cualquier cambio, como por ejemplo de precios, queda de inmediato avisado a todo el personal, incluso a los empleados que en un momento dado pudieran estar de vacaciones.
- Ahorro . el uso del papel queda reducido al mínimo, pudiendo economizarse grandes cantidades de dinero en papelería (a largo plazo más de lo que cuesta la implantación del intranet).
- Acceso . todo el personal puede accesar la información, independientemente de su ubicación física en el momento de consultarla. Existe incluso la posibilidad de tener acceso al servidor de la empresa a través de cualquier otro servidor de Internet, previa identificación del usuario.
- Concentración . todo el personal sabe dónde buscar la información. No necesita ir de oficina en oficina para encontrar los documentos requeridos. Además, todos los datos históricos de las operaciones de la empresa pueden ser buscados en un mismo lugar, simplificándose el establecimiento de contactos con los clientes incluso en caso de cambios de personal.
- Fácil localización y confidencialidad . el uso de ayudas de navegación simplifica notablemente el proceso de localización de documentos, pero a la vez permite un control de quién tiene acceso a qué páginas del Web interno. Existe la posibilidad en un momento dado de impedir el acceso al personal que ha dejado de laborar en la empresa o que por alguna razón ya no ha de visualizar la información.
- Transportabilidad y seguridad . toda la información queda perfectamente ubicada, pudiendo en un momento dado transportar todos los archivos contenidos en un servidor a otro para efectos de respaldo, de seguridad, o incluso de fallas.

.

La seguridad en el intranet

La gran diferencia entre el intranet y otras técnicas de almacenamiento y de comunicación de datos es el hecho de que la información está concentrada en un solo lugar. No ocurre como en algunos sistemas en los cuales cada servidor tiene una copia de la información. Aquí la información está centralizada, evitándose así problemas por actualizaciones hechas a destiempo. Esto no sólo permite el ahorro de espacio en los

servidores, sino que también optimiza todos los procesos de actualización.

En caso de problemas de personal, la simple actualización de las tablas de acceso permite controlar de inmediato quien sí y quién no tiene acceso al servidor, y en caso afirmativo, a qué partes del mismo.

Otra ventaja del intranet es el hecho de que todo el personal opera con las mismas herramientas y con los mismos formatos. Esto permite evitar la duplicidad de información o los errores por presentaciones diferentes de un mismo documento. Además, simplifica los procesos de entrenamiento del personal.

Las técnicas de los exploradores del Web aplicadas a las empresas permiten definir todo tipo de ligas entre páginas o documentos, evitándose entonces la omisión de alguno, o la pérdida de algún detalle.

Los "filtros" o "firewalls" son los elementos de la red que impiden el acceso a los servidores de las empresas desde el Internet cuando dichos servidores están conectados a la red pública. En este sentido, cada día son más las herramientas disponibles en el mercado para mejorar los procedimientos de filtro para impedir el acceso a las redes privadas.

Otra de las ventajas del uso de intranets es la posibilidad de operar con buscadores de documentos, pero también con índices comunes y con imágenes. Esto simplifica notablemente la comunicación y garantiza el manejo de documentación actualizada debidamente controlada por medio de símbolos (por ejemplo de urgente, de confidencial, de interés para x personas, etc.). De esta manera, cualquier comunicación urgente puede ser debidamente marcada y manejada en toda la red, incluso interrumpiendo las labores de los empleados.

SEGURIDAD EN REDES COMPLEJAS: EL CASO DE INTERNET.

El fenómeno de la extensión de la Internet ha adquirido una velocidad tan rápida y unas proporciones, que el panorama actual y muchos de los efectos que se dan en su seno resultan sorprendentes y difícilmente imaginables hace sólo una década.

Inicialmente Internet nace como una serie de redes que promueven el intercambio de información entre investigadores que colaboran en proyectos conjuntos o comparten resultados usando los recursos de la red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Estaba totalmente desaconsejado usarla para el envío de documentos sensibles o clasificados que pudieran manejar los usuarios. situación esta muy comùn, pues hay que recordar que la Internet nace como un contrato del Departamento de Defensa Americano −año 1968− para conectar entre sí tanto las Universidades como los centros de investigación que colaboran de una manera u otra con las Fuerzas Armadas Norteamericanas.

Los protocolos de Internet fueron diseñados de una forma deliberada para que fueran simples yu sencillos. El poco esfuerzo necesario para su desarrollo y verificación jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser echados en falta.

Más recientemente, la conexión a Internet del mundo empresarial se ha producido a un ritmo vertiginoso muy superior a la difusión de ninguna otra tecnología anteriormente ideada. Ello ha significado que esta red de redes se haya convertido en "la red" por excelencia. Esto es, el medio más popular de interconexión de recursos informáticos y embrión de las anunciadas autopistas de la información.

Se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, la cooperación altruista, la práctica política o, simplemente, el juego. En medio de esta variedad han ido aumentando las acciones poco

respetuosas con la privacidad y con la propiedad de recursos y sistemas. *Hackers, frackers, crakers ...* y demás familias han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Además de las técnicas y herramientas criptográficas antes citadas, es importante recalcar que una componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los gestores de la red. Como ejemplo, en la tabla 1 se recoge una lista exhaustiva de problemas detectados, extraída del libro: *"Firewalls and Internet Security. (...)"*.

LISTA DE PELIGROS MÁS COMUNES EN SISTEMAS CONECTADOS A INTERNET	
Fuente: ***"Firewalls and Internet Security. Repelling the Wily Hacker"***	
1.−	De todos los problemas, el mayor son los fallos en el sistema de passwords.
2.−	Los sistemas basados en la autenticación de las direcciones se pueden atacar usando números consecutivos.
3.−	Es fácil interceptar paquetes UDP.
4.−	Los paquetes ICMP pueden interrumpir todas las comunicaciones entre dos nodos.
5.−	Los mensajes ICMP Redirect pueden corromper la tabla de rutas.
6.−	El encaminamiento estático de IP puede comprometer la autenticación basada en las direcciones.
7.−	Es fácil generar mensajes RIP falsos.
8.−	El árbol inverso del DNS se puede usar para conocer nombres de máquinas.
9.−	Un atacante puede corromper voluntariamente la caché de su DNS para evitar responder peticiones inversas.
10.−	Las direcciones de vuelta de un correo electrónico no son fiables.
11.−	El programa sendmail es un peligro en sí mismo.
12.−	No se deben ejecutar a ciegas mensajes MIME.
13.−	Es fácil interceptar sesiones telnet.
14.−	Se pueden atacar protocolos de autenticación modificando el NTP.
15.−	Finger da habitualmente demasiada información sobre los usuarios.
16.−	No debe confiarse en el nombre de la máquina que aparece en un RPC.
17.−	Se puede conseguir que el encargado de asignar puertos IP ejecute RPC en beneficio de quien le llama.
18.−	Se puede conseguir, en muchísimos casos, que NIS entregue el fichero de passwords al exterior.
19.−	A veces es fácil conectar máquinas no autorizadas a un servidor NIS.
20.−	Es difícil revocar derrechos de acceso en NFS.

21.−	Si está mal configurado, el TFTP puede revelar el /etc/passwd.
22.−	No debe permitirse al ftp escribir en su directorio raíz.
23.−	No debe ponerse un fichero de passwords en el área de ftp.
24.−	A veces se abusa de FSP, y se acaba dando acceso a ficheros a quien no se debe dar.
25.−	El formato de información de WWW debe interpretarse cuidadosamente.
26.−	Los servidores WWW deben tener cuidado con los punteros de ficheros.
27.−	Se puede usar ftp para crear información de control del gopher.
28.−	Un servidor WWW puede verse comprometido por un script interrogativo pobremente escrito.
29.−	El MBone se puede usar para atravesar algunos tipos de cortafuego.
30.−	Desde cualquier sitio de la Internet se puede intentar la conexión a una estación X11 (X−Server).
31.−	No se debe confiar en los números de puerto facilitados remotamente.
32.−	Es casi imposible hacer un filtro seguro que deje pasar la mayoría del UDP.
33.−	Se puede construir un túnel encima de cualquier transporte.
34.−	Un cortafuego no previene contra niveles superiores de aquellos en los que actúa.
35.−	Las X11 son muy peligrosas incluso a través de una pasarela.
36.−	Las herramientas de monitorización de red son muy peligrosas si alguien accede ilegítimamente a la máquina en que residen.
37.−	Es peligroso hacer peticiones de finger a máquinas no fiables.
38.−	Se debe de tener cuidado con ficheros en áreas públicas cuyos nombres contengan caracteres especiales.
39.−	Los *caza−passwords* actúan silenciosamente.
40.−	Hay muchas maneras de conseguir copiar el /etc/password
41.−	Registrando completamente los intentos fallidos de conexión, se capturan passwords.
42.−	Un administrador puede ser considerado responsable −si se demuestra conocimiento o negligencia− de las actividades de quien se introduce en sus máquinas.

A la hora de plantearse en que elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

- **Protección de los sistemas de transferencia o transporte.** En este caso, el administrador de un servicio, asume la responsabilidad de garantizar la transferencia segura de la información de forma bastante transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con MTAs seguras, o la instalación de un cortafuego, *(firewall)*, que defiende el acceso a una parte protegida de una red.
- **Aplicaciones seguras extremo a extremo**. Si pensamos por ejemplo en correo electrónico consistiría en construir un mensaje en el cual en contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío, de forma que este mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Aunque el acto de securizar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de su organización. Este mismo planteamiento, se puede usar para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc.

En ambos casos, un problema de capital importancia es la **gestión de claves**. Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. En el caso de las claves secretas el problema mayor consiste en mantener su privacidad durante su

distribución, en caso de que sea inevitable su envío de un punto a otro. En el caso de clave pública, los problemas tienen que ver con la garantía de que pertenecen a su titular y la confianza en su vigencia (que no haya caducado o sido revocada).

Una manera de abordar esta gestión de claves está basada en el uso de los ya citados Certificados de Clave Pública y Autoridades de Certificación. El problema de la vigencia de la clave seresuelve con la generación de Listas de Certifados Revocados (CRLs) por parte de las CAs.

LOS SERVICIOS DE SEGURIDAD

El documento de ISO que describe el Modelo de Referencia OSI, presenta en su Parte 2 una *Arquitectura de Seguridad*. Según esta arquitectura, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes **servicios de seguridad**:

- **Autenticación de entidad par**. Este servicio corrobora la fuente de una unidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una o la otra.
- **Control de acceso.** Este servicio se utiliza para evitar el uso no autorizado de recursos.
- **Confidencialidad de datos.** Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.
- **Integridad de datos**. Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.
- **No repudio**. Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación. Puede ser de dos tipos:
- **Con prueba de origen**. Cuando el destinatario tiene prueba del origen de los datos.
- **Con prueba de entrega**. Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del Modelo de Referencia OSI los siguientes **mecanismos de seguridad**:

- **Cifrado**. El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.

El mecanismo de cifrado soporta el servicio de confidencialidad de datos al tiempo que actúa como complemen to de otros mecanismos de seguridad.

- **Firma digital**. Se puede definir la firma digital como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos. La firma digital supone el cifrado, con una componente secreta del firmante, de la unidad de datos y la elaboración de un valor de control criptográfico.

La firma digital descrita por ITU y OSI en el *Entorno de Autenticación del Directorio* utiliza un esquema criptográfico asimétrico. La firma consiste en una cadena que contiene el resultado de cifrar con RSA aplicando la clave privada del firmante, una versión comprimida, mediante una función hash unidireccional y libre de colisiones, del texto a firmar.

Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

- **Control de acceso.** Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de accesoa recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el enviante está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

El mecanismo de control de acceso soporta el servicio de control de acceso.

- **Integridad de datos.** Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una infomración suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

El mecanismo de integridad de datos soporta el servicio de integridad de datos.

- **Intercambio de autentificación**. Existen dos grados en el mecanismo de autenticación:
- **Autentificación simple**. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.
- **Autentificación fuerte.** Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado.

Un certificado es un documento firmado por una Autoridad de Certificación, válido dunte el período de tiempo indicado, que asocia una clave pública a un usuario.

El mecanismo de intercambio de autenticación se utiliza para soportar el servicio de autenticación de entidad par.

LOS VIRUS

¿Que son?

Antes de saber que son, lo primero que haremos será diferenciar algunos términos que nos pueden conducir a error.

Términos :

- Gusano o Worm

Son programas que tratan de reproducirse a si mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a si mismo.

- Caballo de Troya o Camaleones

Son programas que permanecen en el sistema, no ocasionando acciones destructivas sino todo lo contrario suele capturar datos generalmente password enviándolos a otro sitio, o dejar indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos.

El caballo de troya incluye el código maligno en el programa benigno, mientras que los camaleones crean uno nuevo programa y se añade el código maligno.

- Joke Program

Simplemente tienen un payload (imagen o sucesión de estas) y suelen destruir datos.

- Bombas Lógicas o de Tiempo

Programas que se activan al producirse un acontecimiento determinado. la condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o un estilo técnico Bombas Lógicas), etc... Si no se produce la condición permanece oculto al usuario.

- Retro Virus

Este programa busca cualquier antivirus, localiza un bug (fallo) dentro del antivirus y normalmente lo destruye.

- Virus

Son una combinación de gusanos, caballos de troya, joke programs, retros y bombas lógicas. Suelen ser muy DESTRUCTIVOS.

− La Vida de un Virus

Los virus informáticos tienen un ciclo de vida, que empieza cuando son creados y termina cuando son erradicados completamente. El siguiente resumen describe cada etapa:

- Creación

Hasta unos años atrás, crear un virus requería del conocimiento del lenguaje de programación assembler. Hoy en día, cualquiera con un poco de conocimiento en programación puede crear un virus. Generalmente, los creadores de los virus, son personas maliciosas que desean causar daño a las computadoras.

- Gestación

Luego de que el virus es creado, el programador hace copias asegurándose de que se diseminen. Generalmente esto se logra infectando un programa popular y luego enviándolo a algún BBS o distribuyendo copias en oficinas, colegios u otras organizaciones.

- Reproducción

Los virus se reproducen naturalmente. Un virus bien diseñado se reproducirá por un largo tiempo antes de activarse, lo cual permite que se disemine por todos lados.

- Activación

Los virus que contienen rutinas dañinas, se activarán bajo ciertas condiciones, por ejemplo, en determinada fecha o cuando el usuario haga algo determinado. Los virus sin rutina dañina no se activan, pero causan daño al robar espacio en el disco.

- Descubrimiento

Esta fase por lo general viene después de la activación. Cuando se detecta y se aísla un virus, se envía al International Security Association en Washington D.C, para ser documentado y distribuido a los encargados de desarrollar los productos antivirus. El descubrimiento, normalmente ocurre por lo menos un año antes de que el virus se convierta en una amenaza para la comunidad informática.

- Asimilación

En este punto, quienes desarrollan los productos antivirus, modifican su programa para que éste pueda detectar los nuevos virus. Esto puede tomar de un día a seis meses, dependiendo de quien lo desarrolle y el tipo de virus.

- Eliminación

Si suficiente cantidad de usuarios instalan una protección antivirus actualizada, puede eliminar cualquier virus. Hasta ahora, ningún virus ha desaparecido completamente, pero algunos han dejado de ser una amenaza.

Tipos de virus

- Virus de Acompañante

Estos virus basan su principio en que DOS, ejecuta el primer archivo COM y EXE del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar. Después de ejecutar el nuevo archivo COM creado por el virus y cede el control al archivo EXE.

- Virus de Archivo

Los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es

ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.

Este tipo de virus de dividen el dos:

Virus de **Acción Directa** que son aquellos que no se quedan residentes en memoria y se replican en el momento de ejecutar el fichero infectado y los virus de **Sobrescritura** que corrompen el fichero donde se ubican al sobrescribirlo.

- Bug−Ware

Bug−ware es el termino dado a programas informáticos legales diseñados para realizar funciones concretas. Debido a una inadecuada comprobación de errores o a una programación confusa causan daños al hardware o al software del sistema.

Muchas veces los usuarios finales aducen esos daños a la actividad de virus informáticos. Los programas bug−ware no son en absoluto virus informáticos, simplemente son fragmentos de código mal implementado, que debido a fallos lógicos, dañan el hardware o inutilizan los datos del computador.

- Virus de Macro

De acuerdo con la International Security Association, los virus macro forman el 80% de todos los virus y son los que más rápidamente han crecido en toda la historia de los ordenadores en los últimos 5 años. A diferencia de otros tipos de virus, los virus macro no son exclusivos de ningún sistema operativo y se diseminan fácilmente a través de archivos adjuntos de e−mail, disquetes, bajadas de Internet, transferencia de archivos y aplicaciones compartidas.

Los virus macro son, sin embargo, aplicaciones específicas. Infectan las utilidades macro que acompañan ciertas aplicaciones como el Microsoft Word y Excel, lo que significa que un Word virus macro puede infectar un documento Excel y viceversa. En cambio, los virus macro viajan entre archivos en las aplicaciones y pueden, eventualmente, infectar miles de archivos.

Los virus macro son escritos en Visual Basic y son muy fáciles de crear. Pueden infectar diferentes puntos de un archivo en uso, por ejemplo, cuando éste se abre, se graba, se cierra o se borra. Lo primero que hacen es modificar la plantilla maestra (normal.dot) para ejecutar varias macros insertadas por el virus, así cada documento que abramos o creemos, se incluirán las macros "víricas".

Con la posibilidad de contener un virus convencional, cambiar un ejecutable o DLL e insertarlo en el sistema.

- Mailbomb

Esta clase de virus todavía no esta catalogado como tal pero, os voy a poner un ejemplo de lo que hacen, y haber que opinarías del este tipo de programas si son o no.

Por lo general todos son iguales, escribes un texto que quieras una dirección de e−mail (victima) introduces el numero de copias y ya esta.

El programa crea tantos mensajes como el numero de copias indicado antes, seguidamente empezara a enviar mensajes hasta saturar el correo de la victima.

- Virus del Mirc

Son la nueva generación de infección, aprovechan la ventajas proporcionadas por la Red y de los millones de usuarios conectados a cualquier IRC a través del Mirc. Consiste en un script para el cliente de IRC Mirc. Cuando se accede a un canal de IRC, recibe por DCC un archivo llamado "script.ini". Por defecto, el subdirectorio donde se descargan los archivos es el mismo donde esta instalado el programa, esto causa que el "script.ini" original se sobrescrito por el "script.ini" maligno.

Bueno después de lo dicho nos preguntaremos ¿y para en que nos afecta a nosotros? Pues muy fácil, los autores pueden desconectarte del IRC o acceder a información privada,(archivo de claves o el "etc/passwd" de Linux).

- Virus Multi−partes

Los virus multi−parte pueden infectar tanto el sector de arranque como los archivos ejecutables, suelen ser una combinación de todos los tipos existentes de virus, su poder de destrucción es muy superior a los demás y de alto riesgo para nuestros datos , su tamaño es mas grande a cambio de tener muchas mas opciones de propagarse e infección de cualquier sistema.

- Virus de Sector de Arranque

Este tipo de virus infecta el sector de arranque de un disquete y se esparce en el disco duro del usuario, el cual también puede infectar el sector de arranque del disco duro (MBR). Una vez que el MBR o sector de arranque esté infectado, el virus intenta infectar cada disquete que se inserte en el sistema ,ya sea una CD−R, una unidad ZIP o cualquier sistema de almacenamiento de datos.

Los virus de arranque trabajan de la siguiente manera: se ocultan en el primer sector de un disco y se cargan en la memoria antes de que los archivos del sistema se carguen. Esto les permite tomar total control de las interrupciones del DOS y así, pueden diseminarse y causar daño.

Estos virus, generalmente reemplazan los contenidos del MBR o sector de arranque con su propio contenido y mueven el sector a otra área en el disco. La erradicación de un virus de arranque puede hacerse inicializando la máquina desde un disquete sin infectar, o encontrando el sector de arranque original y reemplazándolo en el lugar correcto del disco.

- Virus del WEB

Los applets de JAVA y los controles Active X, son unos lenguajes nuevos orientados a Internet, pero las nuevas tecnologías abren un mundo nuevo a explotar por los creadores de virus. De momento no son muy utilizados pero a partir del 2000, superaran en numero a los virus de macro.

Síntomas

¿Cuales son los síntomas mas comunes cuando tenemos un virus?

- **Reducción del espacio libre en la memoria o disco duro.**
  Un virus, cuando entra en un ordenador, debe situarse obligatoriamente en la memoria RAM , y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.
- **Frecuentes caídas del sistema operativo.**
- **Las operaciones rutinarias se realizan con mas lentitud.**
- **Aparición de programas residentes en memoria desconocidos.**
- **Tiempos de carga mayores.**
- **Aparición de mensajes de error no comunes.**
- **Fallos en la ejecución de los programas.**
- **Actividad y comportamientos inusuales de la pantalla.**
  Muchos de los virus eligen el sistema de vídeo para notificar al usuario su presencia en el ordenador.

Cualquier desajuste de la pantalla, o de los caracteres de esta nos puede notificar la presencia de un virus.

- **El disco duro aparece con sectores en mal estado**
  Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.

- **Cambios en las características de los ficheros ejecutables**
  Casi todos los virus de fichero, aumentan el tamaño de un fichero ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto, que cambien la fecha del fichero a la fecha de infección.

- **Aparición de anomalías en el teclado**
  Existen algunos virus que definen ciertas teclas que al ser pulsadas, realizan acciones perniciosas en el ordenador. También suele ser común el cambio de la configuración de las teclas, por la del país donde se programo el virus.

Aparte de estos síntomas, lo bueno es que enseguida nos daremos cuenta de que estamos infectados, por una simple razón, nos tiramos horas delante de nuestro ordenado y sabemos a la perfección, cuanto tiempo invierte en hacer una operación, cual es su ritmo de procesamiento, etc. Es decir, conocemos demasiado bien nuestra maquina para no advertir que le pasa algo.

Protéjase

En esta sección, recogemos las cosas que hay que hacer para mantener nuestros datos a salvo de perdidas innecesarias provocadas por los virus o similares.

- Realizar copias de seguridad de los datos importantes. Si efectuamos la copia cada día mejor
- No aceptar software pirata, siempre software y el soporte original.
- Proteger todos los disco contra escritura, sobre todos los del *sistema*.
- Seleccionar el disco duro como arranque por defecto, desde la BIOS para evitar los virus del sector de arranque.
- Escanear todos los disquetes, CD−ROM, CD−R, CD−RW, Discos duros extraíbles unidades ZIP o cualquier otra unidad externa, incluso los discos vacíos, para verificar que están limpios.
- Actualizar el antivirus cada mes desde el web del fabricante.
- No descargar archivos de Internet de identidad dudosa.
- No abrir ningún archivo adjunto en un e−mail, sin antes escanearlo, sobre todo si es un ejecutable.
- Adquiera un antivirus, que haga un escáner de todos los archivos, que se baje de Internet.
- Escanear periódicamente el disco duro desde el disco original del sistema, para evitar que algún virus se cargue en memoria previamente al análisis del antivirus.
- Si tiene instalado el Mirc, desactive la opción *auto get* que recoge los ficheros DCC de forma automática y cambie el subdirectorio por defecto para que sobrescriba el "script.ini" original.