INVESTIGA I+D+i 2011/2012

GUÍA ESPECÍFICA DE TRABAJO SOBRE SEGURIDAD INFORMÁTICA

Texto de D. Francisco Serradilla García

Septiembre de 2011

INTRODUCCIÓN

La seguridad informática, o más recientemente la seguridad de la información, se ocupa de proteger a la información y a los sistemas de información de accesos no autorizados, usos no adecuados, interrupción de servicio y alteración, copia o destrucción de los datos.

Los tipos de protección fundamentales se refieren a la integridad (la información no es modificada sin autorización), la confidencialidad (sólo pueden acceder a ella los usuarios legítimos) y la disponibilidad de la información (evitar que se borre o que el sistema deje de funcionar).

Actualmente vivimos en una sociedad hiperconectada, en la que las amenazas a la seguridad de la información se han multiplicado. Ningún ordenador es completamente seguro si está conectado a la red. De hecho los protocolos militares marcan que un ordenador con información confidencial no sólo no puede estar conectado a la red, sino que ¡debe estar a una distancia mínima de cualquier otro ordenador!

Naturalmente, si ningún ordenador está completamente a salvo, esto no quiere decir que debamos ignorar todo lo relativo a la protección de la seguridad de los ordenadores. Una cosa es que las puertas de una casa se puedan forzar y otra que dejemos siempre la puerta abierta. Así que es importante conocer las amenazas y el modo de dificultarlas, así como los síntomas de que algo va mal y cómo solucionar los problemas.

En resumen, si alguien quiere entrar en un sistema y tiene los conocimientos necesarios, seguramente pueda hacerlo, pero si el sistema está bien protegido quizá le lleve mucho tiempo y además tenga que saber mucho del tema, de modo que el esfuerzo no valdrá la pena a menos que tengamos secretos de seguridad nacional en nuestro ordenador. Por ello vale la pena guardar una serie de precauciones básicas que luego enumeraremos. La seguridad informática es un campo amplio y complejo, pero a nivel doméstico unas pocas

medidas ayudan mucho. El uso de estas medidas contribuirá a dificultar enormemente el acceso no autorizado a usuarios de bajo nivel.

Es falso pensar que para crackear un sistema hay que tener muchos conocimientos. Hay herramientas ya preparadas que basta utilizar como usuario para llevar a cabo muchas de las amenazas que describiremos. Aunque quienes han desarrollado estas herramientas sí tienen por lo general grandes conocimientos del asunto, la mayoría simplemente las utiliza y es bastante ignorante de su funcionamiento. Para hacerse una idea, no es lo mismo "usar Windows" que "haber desarrollado Windows", ¿verdad?

HACKERS Y CRACKERS

El término hacker no tiene en la comunidad informática ninguna carga peyorativa. Es simplemente alguien que sabe mucho de sistemas, y habitualmente utiliza este conocimiento con el fin de proteger estos sistemas. La prensa con frecuencia lo usa en el sentido de cracker, término que sí tiene connotaciones negativas y que se refiere a quien usa esos conocimientos para vulnerar sistemas, escribir virus de ordenador o quitar protecciones anticopia de los programas.

TIPOS DE AMENAZAS

ATAQUES DE DENEGACIÓN DE SERVICIO (ATAQUES DOS)

Cuando miles de ordenadores intentan acceder simultáneamente a un mismo recurso en red, este recurso puede llegar a bloquearse. Los servidores web están dimensionados para soportar una determinada carga de peticiones por segundo. Si este límite se supera el sistema es incapaz de responder adecuadamente y se producen demoras y, eventualmente, la caída del sistema.

Esto puede conseguirse de diversos modos. Unos de ellos es muy simple: no hay más que poner de acuerdo al número de usuarios suficiente para que abran una misma página web una y otra vez. Esto es lo que ha sucedido varias veces en ataques coordinados del grupo Anonymous contra la SGAE y el Ministerio de Cultura, por ejemplo.

Naturalmente hay herramientas que automatizan la realización de peticiones, pero en general no basta con un único ordenador atacando, sino que hay que utilizar varios a la vez.

VIRUS, MALWARE, SPYWARE, TROYANOS Y OTROS "BICHOS"

Todo el mundo sabe lo que es un virus. Básicamente es un tipo de programa que se instala en nuestro sistema sin que lo sepamos para hacer algo malo. Se llama virus porque tiene capacidad de copiarse a sí mismo utilizando los recursos del ordenador que lo hospeda, igual que hacen los virus biológicos con los seres vivos.

Los primeros virus buscaban casi siempre provocar un mal funcionamiento en el ordenador, que solía conducir a la pérdida de datos. Realmente poco podían hacer en provecho de su creador.

Pero cuando la red se populariza los virus pasan a ser una herramienta para ganar dinero de diversas formas: robando datos bancarios o contraseñas, por ejemplo, o permitiendo al creador del virus que entre en nuestro ordenador o que lo utilice para enviar correo basura o provocar ataques de denegación de servicio. Entonces comienza a popularizarse el término malware, que incluye a los virus y a otros tipos de programas fraudulentos.

El término malware (malicious software) se refiere, en general, a "software que hace cosas malas", y en particular está asociado a programas que comunican cosas por la red sin permiso del usuario del sistema.

No pienses que es una cosa rara o que es poco probable que te pase. Según algunos estudios, más de la mitad de los ordenadores en España están infectados por algún tipo de malware.

TIPOS DE MALWARE

Aparte de los virus, ya comentados, los principales tipos de malware son los troyanos, las redes de bots (botnets), el spyware, los gusanos y los keyloggers, entre otros. Las fronteras entre ellos no están claramente definidas, y en algunos casos un mismo malware pertenece a varias de estas categorías.

Un troyano es un programa aparentemente inofensivo, pero que, aparte de la función que aparentemente realiza, esconde, igual que el Caballo de Troya, un secreto. Este secreto suele ser que permite a un usuario remoto abrir una sesión en nuestro ordenador para buscar y descargar archivos (de nuevo el objetivo vuelve a ser la información bancaria o las contraseñas) o instalar otros tipos de malware.

Una red de bots es una red formada por todos los ordenadores que tienen determinado malware que permite al autor tomar el control de esos ordenadores para lanzar ataques de denegación de servicio o para enviar correo basura. Así estos ordenadores infectados son como zombies que obedecen a las órdenes de alguien que no es su usuario legítimo. La mayor

parte del correo basura se envía desde ordenadores de personas normales que están contagiados por algún tipo de malware.

Si el malware está bien escrito y el asaltante lo usa correctamente, el usuario legítimo no notará que el ordenador está haciendo algo además de sus funciones normales, pero este no suele ser el caso. Un síntoma claro de tener instalado malware es que "el ordenador va lento". Lo mejor en estos casos es pasar un antivirus o incluso reinstalar de cero el sistema operativo.

Un gusano es un malware que se copia de una máquina a otra a través de la red.

El objetivo de un keylogger es capturar las pulsaciones de teclado y enviarlas a su creador, que buscará en ellas contraseñas de acceso o información sensible.

Finalmente, el spyware se instala en el ordenador y muestra anuncios cuando se abren páginas web, reportando al atacante los beneficios de la publicidad.

ACCESOS NO AUTORIZADOS

REDES WIFI

Las redes wifi en nuestro país son enormemente inseguras. Con los conocimientos y herramientas adecuadas, es posible obtener acceso no autorizado a la gran mayoría de redes wifi, en tiempos que van desde 1 segundo, en los casos más vulnerables, hasta unos minutos.

Esto se debe a varios factores, entre los que destacan fallos en la implementación del cifrado WEP (el más utilizado) y enormes deficiencias en el modo de proceder de las operadoras (ya que asignan claves por defecto parcial o completamente predecibles, y a veces impiden que el usuario acceda a su propio router para cambiar la clave).

Para tener nuestra red wifi medianamente protegida es preciso usar cifrado WPA que, aunque también puede ser atacado, requiere de un ataque de diccionario que puede demorarse semanas o meses. Si lo que el atacante quiere, como suele ser habitual, es simplemente acceder a Internet, se buscará otra red más sencilla de crackear.

Una medida fundamental para estar más protegidos es cambiar la contraseña por defecto del router, aunque si usamos WEP seguimos siendo muy vulnerables.

Como ejemplo de la debilidad de algunas redes, la clave por defecto de las redes WLAN_XXXX pueden obtenerse con un programas disponibles para iPhone y Android en 1 segundo.

ORDENADORES

Una vez que un atacante esté en nuestra red, puede intentar acceder a los ordenadores que haya en esa red. Contraseñas sencillas o incluso usuarios sin contraseña le facilitarán esta labor. Dentro del ordenador buscarán información sensible, como datos de cuentas bancarias o tarjetas de crédito, por ejemplo. Esta información no debería nunca guardarse en el ordenador, o al menos debería estar cifrada por un programa de confianza.

ESCALADA DE PRIVILEGIOS

Para poder instalar programas o modificar el sistema operativo en un ordenador protegido es necesario autentificarse como administrador. Un ataque común es el denominado "escalada de privilegios", que intenta alcanzar el estado de administrador desde el estado de usuario normal. Para ello lo habitual es utilizar una vulnerabilidad (fallo) de algún programa que necesita en cierto momento funcionar en ese nivel de privilegios.

Un software bien diseñado no debería necesitar este tipo de nivel, pero el desarrollo software es algo tan complejo que en muchos casos no se respeta esta norma. Por poner un ejemplo, en Windows XP era posible realizar una escalada de privilegios simplemente renombrando en programa de terminal, dándole el nombre del programa que se activaba para el acceso de personas con discapacidad. Hecho esto, pulsando tres veces la tecla alt en la pantalla de acceso se nos abría un terminal ¡de administrador!

PHISHING

El phishing es una técnica que se basa en copiar el aspecto de la página original de un sitio legítimo, por ejemplo un banco, y pedir al usuario (con alguna excusa) que introduzca sus datos allí haciéndole creer que es el sitio verdadero. La mayor parte de las veces el phishing se inicia con un mensaje de correo que da la url del sitio falso pero escribe en pantalla la del verdadero.

Si el usuario mete los datos en el sitio falso, los atacantes lo guardan y lo pueden usar para secuestrar la cuenta o estafar al usuario legítimo.

VULNERABILIDADES EN EL SOFTWARE

Todos los programas contienen errores que pueden provocar fallos. En ciertas condiciones, estos fallos pueden utilizarse (con lo que se denomina un exploit) para inyectar código en el programa original y conseguir que este código se ejecute con permisos especiales para con ello modificar el sistema o acceder a información protegida.

Cada vez que se detecta una vulnerabilidad, el programa se corrige y se envía una actualización de seguridad del sistema. Es importante por ello mantener el sistema actualizado.

COPIA DE SOFTWARE

Aunque en España es legal la copia privada de contenidos culturales (música, películas, fotografías, etc.) no lo es la copia de software (lo que incluye juegos de ordenador), salvo que se disponga del programa original, denominándose entonces "copia de seguridad". Esto es bastante desconocido por el ciudadano medio, de modo que gran parte del software instalado en los ordenadores personales es ilegal. Aunque los productores de software intentan evitar que sus programas funcionen cuando se copian ilegalmente, la ingeniería inversa permite saltarse estas protecciones modificando el programa ejecutable.

CARTUCHOS Y MODIFICACIONES DE FIRMWARE

En contra de lo que pueda creerse, estas actividades son legales en nuestro país, siempre que la modificación se realice para añadir funcionalidades extra a los dispositivos, como por ejemplo reproducir contenidos multimedia (películas, fotos, etc). Es decir, venderlos y utilizarlos es legal; lo que no es legal es instalar en ellos una rom de un juego obtenida de modo ilegal (sin haber adquirido el original).

PRIVACIDAD

El acceso a datos de carácter privado está fuertemente protegido por la ley española, pero no es así en todos los países. Empresas como Facebook retienen los datos de carácter privado incluso después del borrado de una cuenta, cosa que es ilegal en nuestro país pero no en su país de origen, Estados Unidos.

INGENIERÍA SOCIAL

En muchos casos el humano es el eslabón más débil en la cadena de la seguridad, empezando por la elección de las claves: un estudio encontró que las claves más utilizadas en lengua inglesa eran "god," "sex", "money" y "love". Actualmente se han añadido otras como "123456" o "password". Existen listas que recogen las claves más utilizadas y que permiten los llamados "ataques de diccionario", que consisten en probar estas contraseñas habituales de modo sistemático contra un servidor o una red.

Otros hábitos, como apuntar la contraseñas en un post-it que se pega al monitor o guardar las contraseñas en un archivo de texto en el propio ordenador son malas prácticas de cara a la seguridad del sistema.

HERRAMIENTAS DE PROTECCIÓN

CONEXIONES SEGURAS (SSL Y VPN)

Actualmente las conexiones no cifradas (http, ftp, telnet, etc.) se consideran muy inseguras. Alguien conectado a nuestra misma red puede utilizar un tipo de programas llamados sniffers para ver la información que viaja por ella. Si por ejemplo introducimos una contraseña, esta contraseña viaja por la red sin cifrar, y puede ser interceptada por este tipo de programas.

Para evitar estos problemas se deben utilizar versiones de estos servicios que envíen la información cifrada, de modo que si alguien usa un sniffer no verá más que información incomprensible. De nuevo, como hemos indicado en otros apartados, con el tiempo y potencia de cálculo suficientes, esta información puede ser descifrada, pero en el caso de un usuario normal el esfuerzo no vale la pena.

Así pues, siempre es recomendable utilizar los programas equivalentes que utilizan SSL (secure sockets layer), el cual establece este nivel de comunicación segura (cifrada) entre servidor y cliente. En general, los servicios seguros incluyen una "s" en su nombre. Por ejemplo, en lugar de http hablamos de https, en lugar de ftp de ftps y en lugar de telnet se usa ssh.

Un modo alternativo de gestionar el cifrado entre el origen y el destino de la información es utilizando una Red Privada Virtual (Virtual Private Network, o VPN), en la que todo el canal se cifra independientemente del protocolo que se use luego sobre el canal.

CRIPTOGRAFÍA

Para construir las conexiones seguras de las que hablamos en los puntos anteriores, se utilizan las técnicas de criptografía, que son las que permiten modificar un mensaje mediante una clave, de modo reversible, para que éste sea ilegible si no se dispone de la clave.

Los primeros sistemas de cifrado inventados por el hombre utilizaban la misma clave para el cifrado y para el descifrado, lo que presentaba un punto débil: de algún modo había que hacerle llegar la clave al receptor del mensaje para que éste pudiera descifrar la información. Si la clave era interceptada por alguien, éste podía descifrar el mensaje, siempre que conociera también el método de cifrado.

En la actualidad se utilizan procedimientos mucho más complejos que se sustentan por el uso de dos claves diferentes: una para cifrar y otra para descifrar. Así, la clave para cifrar la podemos dar a cualquiera que nos quiera enviar un mensaje cifrado, pero sólo podrá descifrarse el mensaje con la clave privada, que no se da a nadie. Ciertos procedimientos matemáticos permiten generar estos pares de claves publica/privada, que están interrelacionadas, pero la clave privada no puede deducirse a partir de la pública (de nuevo, no es que no pueda hacerse, pero el coste computacional y el tiempo necesario puede ser muy elevado, en principio tanto como queramos si las claves son suficientemente largas).

Así, si alguien intercepta la clave, podrá enviar un mensaje cifrado al receptor, pero no descifrar los que otros envíen.

Curiosamente, este mismo procedimiento sirve para la firma digital, es decir, para estar seguros de que un mensaje proviene de un remitente determinado. Para ello el mensaje se cifra con la clave privada y cualquiera que quiera leerlo puede utilizar la clave pública, pero como sólo nosotros conocemos la clave privada quien lea el mensaje se asegura de que éste proviene de nosotros, ya que si no no habría podido descifrarse con la clave pública suministrada.

Los sistemas de clave publica/privada fueron inventados en 1976 por Whitfield Diffie y Martin Hellman.

En los sistemas modernos de cifrado y descifrado los algoritmos son públicos, la seguridad reside exclusivamente en la clave. Naturalmente las claves son muy largas, de 128 bits o más, de modo que los ataques por fuerza bruta (probar todas las claves) llevarían siglos para completarse en las máquinas actuales. Por ejemplo, para una clave de 128 bits, habría que comprobar 2^{128} claves. Esto quiere decir que aunque pidiéramos probar 1000 claves por segundo tardaríamos unos $i10^{28}$ años en probarlas todas!

ANTIVIRUS

Los programas antivirus son sobradamente conocidos, y su uso es imprescindible en sistemas Windows. Lo que no es tan conocido es que hay antivirus gratuitos que nos protegen bastante bien, por ejemplo avgfree o avast. El problema de los antivirus de pago es que vienen instalados por defecto, y cuando al cabo de unos meses caduca su licencia, el usuario cree que sigue estando protegido y sin embargo ya no lo está.

Para que un antivirus sea efectivo hay que actualizar su base de datos periódicamente, ya que cada día aparecen nuevos virus.

CORTAFUEGOS (*FIREWALLS*)

Un cortafuegos es básicamente un filtro que impide que un programa no autorizado acceda a la red. Por ejemplo, si nos instalamos un programa de retoque fotográfico y este quiere acceder a la red, ¿para qué quiere hacerlo? Es como mínimo sospechoso. Si no hemos dicho explícitamente que ese programa puede acceder a la red (ya que por ejemplo si es un navegador debe poder hacerlo) el cortafuegos lo impedirá.

Los cortafuegos también pueden prohibir la comunicación en sentido contrario, es decir, que desde la red se acceda al ordenador.

HERRAMIENTAS DE AUDITORÍA DE SEGURIDAD

Aunque parezca increíble, los Sistemas Operativos actuales traen pocas herramientas que nos permitan saber si alguien está accediendo a nuestro sistema o red. En parte se debe a que estas mismas herramientas pueden ser utilizadas para el propósito contrario. Por ejemplo, los mismos programas que nos permiten descifrar la clave de una red wifi pueden utilizarse para saber si hay alguien no autorizado conectado a nuestra red, lo cual es el primer paso para tomar medidas: saber que nuestro sistema ha sido vulnerado.

En general estas herramientas se denominan "de auditoría de seguridad", y pueden ser utilizadas para auditar la seguridad o para vulnerarla.

MALOS HÁBITOS

Hay algunos malos hábitos que pueden conducir a que se vulnere la seguridad de nuestro ordenador. Para evitarlos es conveniente seguir estas indicaciones:

- No dejar la cuenta de usuario sin contraseña, o con una contraseña trivial. Para evitar ataques de diccionario las contraseñas deben tener letras y números.
- No usar la misma contraseña en muchos sitios, ya que si alguien la obtiene podrá acceder a todos ellos.
- Desactivar el inicio rápido de sesión.
- Cambiar la contraseña por defecto en la red wifi.
- Cambiar la contraseña por defecto del router.
- No instalar programa de procedencia no fiable (por ejemplo bajado de la red de un sitio que no sea el del desarrollador del programa). Si un programa nos pide la contraseña de usuario al instalarse es porque quiere escribir en alguna carpeta del sistema. En ese caso lo mejor es no instalar el programa, salvo que estemos absolutamente seguros de su procedencia.
- No dar datos bancarios o de tarjeta de crédito en un sitio que no sea fiable.
- No introducir contraseñas o información confidencial en sitios no seguros (cuya url no empiece por https).

- No dejar información de contraseñas o datos bancarios en el ordenador sin cifrar.
- Cifrar con un programa confiable.
- No dejar información de contraseñas o datos bancarios en un papel junto al ordenador.
- Nunca introducir contraseñas o datos bancarios en un ordenador no confiable, por ejemplo, en un cibercafé.
- Procurar no dejar el ordenador abierto (dentro de la cuenta de usuario) en lugares donde algún extraño pueda acceder a él. Lo mejor es configurar el salvapantallas para que nos pida la clave al desactivarse.
- No instalar cracks para que funcionen programas piratas (el crack puede hacer otras cosas además de piratear el programa).
- Nunca usar por defecto una cuenta con permisos de administrador. Es mejor usar cuentas limitadas.
- El navegador web es uno de los puntos más vulnerables del equipo. En general se desaconseja utilizar Internet Explorer. Es recomendable instalar Firefox o Chrome, y mantenerlos siempre actualizados.
- Cuidado con los complementos del navegador. Nunca instalar un complemento de un sitio que no sea el del desarrollador. Cuidado con Flash: nunca instalar una actualización de Flash que no sea desde el sitio web de Adobe.
- Nunca enviar claves ni datos bancarios por correo electrónico.
- Instalar siempre las actualizaciones del Sistema Operativo.
- Cuidado al enchufar el pendrive de un amigo. Una vía habitual de contagio, aparte de la red, son los pendrives. En particular son peligrosos los ordenadores donde muchos usuarios enchufan sus pendrives: cibercafés, aulas de informática, etc.
- Cuando instales un programa gratuito, fíjate bien en las cosas que pregunta; en muchos casos te están pidiendo permiso para instalar una barra de búsqueda en el navegador, que no es otra cosa que un spyware. Contesta siempre que no quieres ese complemento. Si tienes ya barras de búsqueda instaladas en el navegador, elimínalas.
- Nunca seguir un enlace desde un correo electrónico (especialmente si no conocemos al autor del correo). Mejor cortar y pegar el texto del enlace en la barra de direcciones del navegador.
- Si el ordenador va lento, no lo dejes estar; es muy posible que tengas algún tipo de malware.
- Si usas Windows, tener siempre antivirus instalado y actualizado. Mejor aún no usar Windows...

REFERENCIAS

http://es.wikipedia.org/wiki/Malware
http://en.wikipedia.org/wiki/Information_security
http://en.wikipedia.org/wiki/Cryptography
http://www.intypedia.com/?lang=es
http://www.itcio.es/amenazas-vulnerabilidades/noticias/1006700016702/mas-mitad-pcs-espana-infectados.1.html