Seguridad Informática

19/08/2010
Maestría en Tecnología de Cómputo
Eduardo Rodriguez

Introducción a la seguridad informática

1.- Introducción

Veamos una serie de casos para ver cómo está el mundo de la seguridad informática…

19 de Enero de 2001

Un intruso borra la página web de la Presidencia de Bulgaria.

25 de Enero de 2001

Denegación de servicio de las páginas web de Microsoft en los Estados Unidos y Europa.

Febrero 2001

Cientos de empresas austríacas sufrieron robos de datos que permitieron a los crackers hacer llamadas telefónicas a lugares de todo el mundo, a cuenta de dichas empresas, por supuesto.

4 de Febrero de 2001

Los sistemas del Foro Económico Internacional, reunido en Davos, fueron invadidos por intrusos. Consiguieron información altamente confidencial y con el número de las tarjetas de crédito de los más altos mandatarios mundiales.

9 de Marzo de 2001

Crackers rusos y ucranianos consiguieron cerca de un millón de números de tarjetas de crédito robadas de las bases de datos de bancos norteamericanos y empresas de comercio electrónico por Internet.

Abril de 2001

Durante la crisis desatada por el avión-espía norteamericano, hackers chinos paralizaron por lo menos veinte sitios web, entre ellos el de la Casa Blanca.

24 de Junio de 2001

El virus CodeRed ya ha producido daños por un valor estimado en 1.200 millones de dólares.

14 de Octubre de 2001

Tras el atentado a las Torres Gemelas, hackers iraníes mantienen paralizada buena parte de la red informática que brinda servicios a General Electric.

21 de Noviembre de 2001

En los EE.UU. atacantes desconocidos entraron en el sitio Web de Playboy. Consiguieron tener acceso a los datos de los usuarios, incluyendo los números de las tarjetas de crédito.

Escenario típico:

"¿Quién va a querer atacarme, si no tengo nada importante?"

Es un error este planteamiento: todo sistema es extremadamente valioso como plataforma de ataque contra otro sistema verdaderamente importante. (Ejemplo: hacker utiliza el ordenador de Juan Pérez para entrar a Banamex).

2.- Seguridad Física

En muchos textos y manuales sobre Seguridad Informática se habla de la seguridad física concerniente a la ubicación de los servidores, los accesos físicos a las máquinas, etc. Aunque es seguridad relacionada con la informática, esas medidas deben ser trabajadas conjuntamente con un ingeniero o arquitecto que diseñe edificios seguros y el especialista en Seguridad Informática.

Como ejemplos de las posibilidades en cuanto a la intrusión a nivel físico, analizaremos dos aspectos:

- El cifrado de datos almacenados en soporte físico (pgpdisk, FSs esteganográficos).
- Captura de emisiones residuales de nuestros equipos (tempest).

A pesar de todas las trabas que podamos poner para que un soporte no sea físicamente suplantado o robado, la realidad es que muchos ataques se producen mediante la manipulación física de los soportes de los datos. (Ejemplo: montar un disco duro desde un Sistema Operativo al que tenemos

acceso total (trinux)). Para evitar este tipo de ataque es recomendable cifrar los datos. Una opción comercial para hacer esto es usar, por ejemplo, PGPDisk, integrada en la Suite PGP de NAI. Para UNIX tenemos CFS y TCFS (Cyphered File System y Transparent Cyphered File System), que ofrecen una encriptación fuerte mediante el empleo de llaves distribuidas (cada usuario tiene una parte de la llave, y se comprueba que su parte está dentro de la llave de protección).

El caso más espectacular en cuanto a cifrado de datos físicos es el de los sistemas de ficheros esteganográficos, como el StegFS. En estos sistemas de protección existen varias claves que permiten el acceso a varios niveles de protección dentro del sistema de ficheros. Alguien que consiga una de las claves, nunca tendrá la certeza sobre si está accediendo a todo el sistema de ficheros o sólo a una parte. De esta manera, aunque alguien fuerce a otro a proporcionarle la clave del sistema (Ejemplo: escenario policial), nunca podrá saber si a lo que está accediendo es a una parte del sistema o a todo.

Existen varias implementaciones más extrañas de sistemas de ficheros esteganográficos, como el ScreamFS, que guarda información confidencial en los bits menos significativos de ficheros de audio.

Otro punto que puede sorprender a quien no esté habituado a sistemas seguros es el hecho de que las radiaciones que emiten todos los dispositivos electrónicos, pueden capturarse y analizarse.

Un programa de ejemplo muy impactante es el Tempest. Mediante cambios en la frecuencia del monitor y utilizando imágenes extrañas, es capaz de emitir música que puede ser captada por una radio AM sencilla.

Tempest es sólo una prueba de concepto, pero demuestra que lo que muestran nuestros monitores puede ser captado sin mucho esfuerzo por un receptor potente. Tempest permite incluso reproducir MP3s desde el monitor, pero existen además dispositivos capaces de captar las corrientes de 5 voltios que discurren por el cable del teclado, u otros dispositivos.

3.- Seguridad en el SO

Una vez analizada la seguridad física, conviene detenerse en examinar el grado de seguridad de nuestros Sistemas Operativos, y los factores que influyen en la pérdida de su seguridad:

3.1.- Fallos en la configuración

Muchos de los ataques se producen por fallos en las configuraciones, a pesar de usar SOs "inherentemente seguros".

Los fallos en la configuración del sistema pueden deberse a dos razones:

- Configuraciones por defecto inseguras (revisar por ejemplo la Bugtraq). Ejemplos característicos de este tipo de errores podrían ser:
  - listado de directorios en httpd's (IIS o versiones antiguas de Apache)
  - passwords por defecto (ejemplo: routers de enlaces telefónicos: adminttd/adminttd)

- por negligencia del administrador, como por ejemplo:
  - no preocuparse de borrar los ficheros de backup que crean editores como emacs o ultraedit por defecto. Normalmente no se aplican las restricciones o ejecuciones a esos ficheros y son altamente vulnerables (Ejemplo: login.asp.bak).
  - Un administrador prefiere una configuración poco restrictiva y que funcione, que una configuración muy restrictiva y afinada, que pueda provocarle discusiones con sus usuarios.

3.2.- Ingeniería social

Otro factor que influye en la seguridad de un SO es el grado de permeabilidad de sus usuarios promedio a la llamada "Ingeniería Social".

En la Ingeniería Social (literalmente traducido del inglés Social Engineering) se encuentran comprendidas todas aquellas conductas útiles para conseguir información de las personas del entorno de un ordenador. Se tratan de engaños, cuyo método puede tener un carácter externo o

interno al propio sistema informático. (Ejemplos: externo: entrar en el edificio como periodistas, aprovechando la vanidad de la gente; interno: aprovechar la confianza del usuario, como por ejemplo el gusano “Kournikova” o el “I Love You”).

Estos ataques no tienen dificultad técnica, sino grandes dosis de ingenio por el lado del atacante ingenuidad del atacado.

3.3.- Características de un SO seguro

Existen diferentes Sistemas Operativos con compromisos variables con la seguridad. Windows 95/98/Me no fueron diseñados para ser Sistemas Operativos orientados a la red. Los añadidos que sufrieron para hacer posible su interconexión, han ido acompañados de un penoso historial de seguridad. Windows NT, Server, XP y sucesores están orientados a trabajo en red, sin embargo, ya es proverbial la abundancia de huecos de seguridad de los productos de Microsoft. Linux, al igual que la mayoría de los UNIX, fue concebido para facilitar la interoperabilidad entre múltiples usuarios y múltiples máquinas. No es un sistema enfocado en la seguridad, por lo que las afirmaciones que proclaman que Linux es inherentemente seguro no son ciertas. Linux “tiene la

capacidad de ser extremadamente seguro", pero muchas veces esa capacidad no se desarrolla. Otros sistemas operativos como OpenBSD, nacieron con la seguridad con objetivo fundamental en su diseño, por lo que su empleo garantiza un nivel de seguridad muy superior a los anteriores.

Hoy en día es ridículo montar un sistema en un SO sin un diseño orientado a la protección de datos y memoria en un entorno multiusuario real, y carente de funcionalidades de red seguras nativas. (Ejemplo: conservar un servidor web en Windows'98 o ME, solo porque "sigue funcionando").

3.4.- Contraseñas en un SO

Es necesario definir una política de contraseñas adecuada para nuestros sistemas. Si no lo hacemos, de nada servirá toda la protección que añadamos al sistema de contraseñas. (Ejemplo: usar RSA de 8192 bits y usuario "juan", contraseña "juan"). Dicha política deberá centrarse en varios aspectos:

- longitud mínima de la clave.
- complejidad mínima de la clave.
- algoritmo(s) utilizado(s).

- política de caducidad de las claves (cada cuánto tiempo, cuántas contraseñas se recordarán, etc.).

Existen diferentes algoritmos para almacenar las claves. Lo fundamental es que se traten de algoritmos “only-one-way”, es decir, que no sean reversibles, y que sean resistentes al criptoanálisis incremental y diferencial. La potencia de la protección está en función del tiempo empleado para comprobar una clave, y para comprobar todas las posibles claves (éste a su vez en función del algoritmo y la clave empleados).

Algunos SOs y administradores de sistemas utilizan las mismas herramientas para conseguir contraseñas que emplean los intrusos, para realizar auditorías de seguridad en cuanto a las características de las claves de los usuarios del sistema. Los programas que se emplean para conseguir contraseñas se denominan “crackers” y suelen emplear fuerza bruta (tanto mediante un enfoque incremental, como por un ataque mediante diccionario) y algunas técnicas heurísticas bastante elementales (Ejemplo: contraseñas en WinNT, 7 + 7).

4.- Técnicas de ataque

En este apartado veremos algunas de las técnicas utilizadas por los hackers y crackers para atacar sistemas. Unas técnicas que no solo debieran ser conocidas por aquel que pretende atacar un sistema sino también por aquel que pretende defenderlo. Con defensor de un sistema no solo se ha de entender a un administrador de sistemas o un consultor de seguridad sino también a un programador. La mayoría de las técnicas que veremos están basadas en fallos cometidos por los programadores a la hora del implementar el programa.

El administrador de un sistema será responsable de mantener unas buenas políticas de seguridad, una correcta configuración del sistema y de mantenerlo actualizado parcheándolo periódicamente. Sin embargo un administrador de sistemas nunca podrá llegar a tener la certeza de que los programas que componen el sistema operativo del servidor así como programas adicionales, estén libres de bugs. Lo único que el administrador podrá hacer al respecto será mirar todos los días las listas de distribución de seguridad (bugtraq) atento para aplicar los parches tan pronto sean publicados. El programador es por tanto el responsable de escribir código seguro evitando que su

programa sea vulnerable y para ello es de vital importancia que esté familiarizado con los distintos tipos de técnicas de ataque existentes.