Anexo IV

Vulnerabilidades más críticas de los sistemas informáticos

Álvaro Gómez Vieites

ANEXO IV

VULNERABILIDADES MÁS CRÍTICAS DE LOS SISTEMAS INFORMÁTICOS

LAS 20 VULNERABILIDADES MÁS CRÍTICAS SEGÚN THE SANS INSTITUTE

Esta lista con las 20 vulnerabilidades de seguridad más críticas en Internet, publicada por The SANS Institute[1] (http://www.sans.org/top20/), se ha convertido en una auténtica guía de referencia sobre los problemas de seguridad más habituales, ya que analiza aquellos problemas de seguridad que son más utilizados en los ataques contra sistemas informáticos, así como las vulnerabilidades empleadas por los gusanos y virus de propagación masiva como mecanismo de infección de los equipos.

Las 10 vulnerabilidades más críticas de los sistemas Windows

W1. Existencia de servidores Web y sus servicios asociados

Cuando se instala un servidor Web en un equipo Windows, en su configuración por defecto se activan algunos servicios y/o configuraciones que son

[1] The SANS Institute (*SysAdmin, Audit, Network, Security Institute*, www.sans.org) es una organización especializada en la formación técnica sobre seguridad informática que comenzó a publicar esta lista en 1999.

vulnerables a diversos tipos de ataques, que van desde la denegación de servicio hasta el compromiso total del sistema. Si la máquina debe actuar como servidor Web, es preciso verificar que la versión del mismo ha sido actualizada, se ha revisado la configuración y se han desactivado los servicios innecesarios.

Así, por ejemplo, la vulnerabilidad conocida como "*Web Server Folder Traversal*" permitía ejecutar código en los servidores Internet Information Server de Microsoft a través de una determinada petición Web maliciosa (petición GET que trataba de tener acceso al intérprete de comandos del sistema: "CMD.EXE"). Esta vulnerabilidad pudo ser utilizada por virus como Nimda para tomar el control del servidor Web e instalar archivos con contenido dañino dentro del sistema. Microsoft publicó el parche para resolver este problema en octubre de 2000.

W2. Servicio Workstation de Windows

Existe una vulnerabilidad de desbordamiento de memoria en el servicio Workstation de Windows 2000 y Windows XP, que puede ser utilizada por un usuario remoto para forzar la ejecución de código en los sistemas vulnerables. Este código se ejecutará en el contexto de seguridad de la cuenta del sistema (usuario "System"), lo que permite un acceso con los máximos privilegios en el ordenador comprometido.

W3. Servicios de acceso remoto de Windows

Todas las versiones de Windows incluyen mecanismos para facilitar el acceso remoto a las unidades de disco y al registro del sistema, así como para la ejecución remota de código. En estos servicios se han descubierto numerosas vulnerabilidades que han sido explotadas por distintos gusanos y virus para propagarse a través de las redes Windows.

W4. Microsoft SQL Server

En los últimos años se han publicado varias vulnerabilidades del gestor de bases de datos SQL Server de Microsoft, algunas de ellas consideradas como críticas, ya que pueden ser utilizadas para acceder y/o modificar a la información almacenada en las bases de datos de la organización, así como para facilitar la propagación de virus y gusanos a través de redes (como en el caso del famoso gusano "Slammer", que tuvo un gran impacto en Internet en 2003).

W5. Autenticación de Windows

Muchos equipos Windows todavía presentan importantes deficiencias en sus mecanismos de autenticación: existencia de cuentas sin contraseña o con contraseñas ampliamente conocidas o fácilmente deducibles, por ejemplo. También es frecuente que diversos programas o incluso servicios del propio sistema operativo creen nuevas cuentas de usuario con un débil mecanismo de autenticación. Por otra parte, si bien algunos de los protocolos de autenticación de Windows transmiten las contraseñas encriptadas a través de la red, sólo el protocolo NTLMv2 ha demostrado ser bastante

seguro, por lo que se deberían descartar otros protocolos anteriores (como NTLM), ya que resultan bastante vulnerables frente a ataques de fuerza bruta.

W6. Navegadores Web

Los navegadores utilizados para acceder a servicios como el World Wide Web constituyen otro de los puntos débiles de seguridad, debido a las numerosas vulnerabilidades detectadas. Internet Explorer es el navegador para el que se han publicado más actualizaciones y parches de seguridad, pero también se han encontrado numerosas vulnerabilidades que afectan a otros navegadores como Opera, Mozilla, Firefox o Netscape.

En concreto, la vulnerabilidad "IFRAME" de Internet Explorer ha tenido una especial incidencia, ya que posibilita la ejecución automática del contenido y los ficheros adjuntos de un correo electrónico HTML (el visor por defecto de estos correos HTML es el navegador instalado en el equipo) con tan sólo visualizar un mensaje infectado por un virus, sin necesidad de que el usuario abra el mensaje de correo. Los detalles de esta vulnerabilidad fueron publicados en marzo de 2001, siendo explotados posteriormente por virus como el "Nimda" (septiembre 2001).

W7. Aplicaciones para compartir archivos

Algunas aplicaciones populares para compartir archivos (servicios P2P) presentan serios problemas de seguridad que pueden ser utilizados por un atacante para obtener el control del ordenador del usuario. Otro riesgos habituales son los diversos programas espías ("*spyware*") incluidos en algunas de las aplicaciones más populares de compartición de archivos. Por otra parte, en los últimos años se han utilizado las redes P2P como un nuevo mecanismo para la propagación de virus y gusanos.

W8. Subsistema LSAS

El subsistema LSAS (*Local Security Authority Subsystem*) de Windows 2000, Windows Server 2003 y Windows XP es vulnerable a diversos ataques de desbordamiento de memoria que pueden permitir a un atacante remoto obtener el control completo del sistema vulnerable. Esta vulnerabilidad ha sido explotada por gusanos como el "Sasser" (mayo de 2004) para propagarse de forma muy rápida a través de los equipos conectados a Internet. "Sasser" podía infectar a todos los sistemas Windows 2000 y Windows XP que no habían aplicado el parche de seguridad "MS04-0112" que Microsoft distribuyó en abril de 2004.

W9. Lector de correo

Algunos de los lectores de correo más populares de los sistemas Windows, como Outlook Express, también han demostrado ser bastante inseguros, sobre todo cuando no han sido convenientemente actualizados con los últimos parches de seguridad y su configuración no es la más adecuada. Las vulnerabilidades de Outlook

Express han facilitado la introducción de virus en el sistema (sin que sea necesario ejecutar ningún programa o fichero adjunto a un mensaje de correo) y la sustracción de información sensible.

W10. Sistemas de mensajería instantánea

Los diversos programas de mensajería instantánea, como el Instant Messenger o Yahoo Messenger, pueden ser víctimas de ataques realizados de forma remota para tratar de obtener el control de los equipos vulnerables. Por este motivo, es fundamental que el usuario de estas aplicaciones haya instalado las últimas actualizaciones de seguridad.

Las 10 vulnerabilidades más críticas de los sistemas Unix/Linux

U1. Software BIND

BIND es uno de los servidores de nombres de dominio (DNS) más utilizado en sistemas UNIX, constituyendo un servicio de gran importancia para el correcto funcionamiento de Internet, ya que se encarga de la traducción de los nombres de dominio a sus correspondientes direcciones IP. Sin embargo, varias versiones de BIND presentan vulnerabilidades que pueden ser utilizadas por un atacante remoto para comprometer el servidor DNS. Además, en muchas redes los servidores DNS han sido configurados de forma poco robusta, de modo que pueden revelar información sensible a terceros sobre la topología y los servicios de la red.

U2. Servidor Web

El servidor Web más utilizado en los sistemas Unix y Linux es el servidor Apache, el cual también se ha visto afectado por distintas vulnerabilidades, así como por una configuración inadecuada por parte de los responsables del servidor Web. Por este motivo, SANS Institute señala la importancia de revisar su configuración y de aplicar los últimos parches y actualizaciones de seguridad publicados.

U3. Autenticación

También resulta bastante frecuente encontrar equipos Unix con deficiencias en sus mecanismos de autenticación: existencia de cuentas sin contraseña o con contraseñas ampliamente conocidas o fácilmente deducibles.

U4. Sistemas de control de versiones

El sistema de control de versiones más utilizado en entornos Unix es CVS. Si la configuración del servidor CVS permite conexiones anónimas, determinadas versiones son vulnerables a ataques de desbordamiento de memoria que pueden ser utilizados para ejecutar código arbitrario en el servidor.

U5. Servicio de transporte de correo

El servicio de transporte de correo de los equipos UNIX también presenta distintas vulnerabilidades, que podrían permitir a un atacante externo tomar el control del equipo para distribuir correo basura (*spam*) o para robar información sensible de los usuarios de este servicio.

U6. Protocolo SNMP

El protocolo SNMP se utiliza para la gestión y configuración remota de los distintos dispositivos conectados a una red, como las impresoras, los ordenadores o los *routers* y otros elementos de conectividad. Sin embargo, las primeras versiones del protocolo SNMP cuentan con unos mecanismos de autenticación muy poco robustos, por lo que resultan vulnerables a varios tipos de ataques, que podrían provocar una modificación no autorizada de la configuración de estos dispositivos o incluso llevar a cabo una denegación de servicio (DoS).

U7. Librería OpenSSL

En los últimos años se han detectado varias vulnerabilidades en la librería OpenSSL[2], que afectan a un gran número de productos que emplean algunas de las funciones incluidas en dicha librería: el servidor Web Apache, CUPS, Curl, OpenLDAP o el servidor de correo Sendmail, entre otros. Por este motivo, conviene comprobar que en el equipo UNIX se está empleando la versión más reciente de la librería OpenSSL.

U8. Mala configuración de los servicios de red

Los equipos UNIX suelen emplear los servicios NFS (*Network File System*) y NIS para poder compartir recursos e información con otros equipos a través una red. Sin embargo, una mala configuración de estos servicios puede abrir la puerta a distintos tipos de ataques, que van desde la ejecución de código no autorizado en los sistemas vulnerables hasta la realización de ataques de denegación de servicio (DoS).

U9. Gestores de bases de datos

Los sistemas UNIX también presentan problemas de seguridad motivados por una inadecuada configuración de los gestores de bases de datos instalados en estos equipos, así como por una deficiente política de control de acceso, poniendo en peligro la confidencialidad y disponibilidad de los datos.

[2] Librería que incluye una serie de funciones para poder establecer conexiones seguras mediante algoritmos criptográficos.

U10. Núcleo del sistema operativo

El núcleo del sistema operativo se encarga de realizar funciones básicas para el equipo como el control de la utilización del hardware, la planificación del procesador (CPU), la gestión de la memoria, la comunicación entre procesos y el control de la ejecución de tareas. Se trata, por tanto, de un componente esencial para garantizar el correcto funcionamiento del equipo. Sin embargo, en los últimos años se han descubierto diversas vulnerabilidades en el núcleo de los sistemas UNIX y LINUX que pueden provocar graves problemas de seguridad que afecten a todos los demás componentes del sistema. Por este motivo, es muy importante la correcta configuración del núcleo y su actualización con los últimos parches de seguridad, para evitar las posibles vulnerabilidades del sistema.

REFERENCIAS DE INTERÉS

- ✓ SANS Institute: http://www.sans.org/
- ✓ CERT: http://www.cert.org/
- ✓ EsCERT: http://escert.upc.es/