Control de Integridad en Sistemas operativos

Álvaro Roldán

División de Seguridad de Germinus

Tras la instalación y puesta en funcionamiento de un sistema operativo, es más que recomendable realizar una revisión periódica para determinar si éste ha sido modificado. Una modificación no controlada de un sistema operativo puede suponer dos cosas: o bien que algún usuario o administrador de éste ha realizado cambios no controlados o documentados, o bien que se ha producido una intrusión en el mismo. Un sistema de verificación de integridad nos permitirá descubrir de forma rápida si alguna parte del sistema se ha visto modificada.

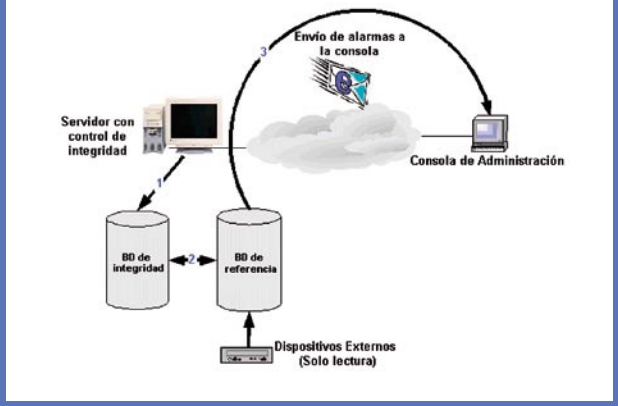
Así pues, una herramienta de control de integridad es aquella que verifica, contrastando con una base de datos de hechos conocidos, el estado de un sistema para determinar los cambios que en él se han producido. Si bien se puede tratar de una herramienta útil para la gestión de configuraciones, su aplicación al mundo de la seguridad viene derivada de su capacidad para detectar ataques producidos a un sistema ya que, en la gran mayoría de los casos, un intruso realizará cambios en el sistema que dicha herramienta de control de integridad podrá detectar. Aunque en algunos casos pueda ser dudosa la intrusión porque, al fin y al cabo, el sistema operativo puede modificarse a sí mismo durante su propio funcionamiento; en otros casos, en los que la pérdida de integridad del sistema es notoria, se presenta un claro síntoma de que tanto el sistema como la seguridad del mismo se ha visto alterada y superada por un usuario malicioso o un intruso.

Las herramientas de control de integridad también pueden utilizarse para un análisis post-mortem de un equipo. Su uso se extiende más allá, pudiéndose utilizar para realizar un análisis forense de un sistema que se haya visto comprometido. Esto se debe a que la herramienta podrá proporcionar gran cantidad de información: ficheros creados, modificados o borrados, variaciones en el contenido de ficheros, etc. Esto puede ser útil para conocer "el qué" y "el cómo" del ataque sufrido (el "por qué" es más difícil de determinar), lo que permite hacerse una idea del ataque y sus consecuencias, aportando información suficiente para evitar en gran medida que hechos así se vuelvan a producir.

Sea cual sea el uso que le demos a este sistema de verificación, el procedimiento para llevar a cabo un control exhaustivo de la integridad del sistema será siempre el mismo para la mayoría de los sistemas operativos. Se basa el procedimiento en unos sencillos pasos:

- ✔ Generar una base de datos de integridad tras la instalación del sistema. Esta información servirá de referencia posteriormente y deberá excluir aquellos archivos que se verán modificados de manera habitual, por procesos propios del sistema (archivos de registro, archivos de colas, ubicaciones temporales, etc.). Esta base de datos deberá almacenarse en un medio físico de sólo lectura (para impedir su modificación posterior).
- ✔ Periódicamente se deberá generar una nueva base de datos y contrastar ésta con la base de datos de referencia, para verificar lo posibles cambios que se han producido en el sistema.
- ✔ Regenerar la base de datos de referencia cuando se realice una tarea administrativa (instalar parches, realizar cambios a la configuración del sistema).

La forma habitual de realizar la comprobación, como se muestra en la "figura 1", es implementarla a través de una tarea automatizada que se realiza por el propio sistema y genera alarmas dirigidas al responsable de seguridad (generalmente serán por correo electrónico) para que éste analice los cambios detectados. Si la diferencia que hay entre ambas bases de datos es muy significativa, serán indicios suficientes de un posible ataque con éxito al sistema. Si bien esto puede ser útil para implementar un mecanismo de detección de intrusos basado en host, nunca hay que olvidar que un intruso



Pasos para el control automatizado de integridad de sistemas Herramientas

suficientemente capaz podrá subvertir este mecanismo de detección, por ejemplo modificando la base de datos de referencia (si ésta no se almacena en un medio físico que no permita modificaciones), deteniendo el control de integridad, instalando un troyano en el sistema de control de integridad utilizado, o, incluso, modificando partes del sistema operativo para que engañen al sistema de control de integridad.

Actualmente existen muchas herramientas distintas que permiten controlar de forma exhaustiva la integridad de un sistema. Todas ellas se rigen por la misma manera de actuar y sus diferencias pueden variar en los mecanismos de comprobación (ligados a diferentes técnicas de hashing), en funcionalidades adicionales (registros almacenados, históricos, interfaces de administración, sistemas de alarma) o en su soporte de distintos sistemas operativos.

Dentro de las herramientas utilizadas para este fin, la más conocida sin duda es Tripwire, un desarrollo del proyecto COSAT de la Universidad de Purdue. Esta herramienta está disponible bajo licencia libre, aunque la empresa Tripwire ofrece versiones propietarias con funcionalidades adicionales y también ofrece herramientas de control de integridad para entornos más especializados (dispositivos de red). Además de Tripwire, existen otras alternativas con licencia de software libre como Integrit, Samhain, Osiris, Syscheck, Aide y Fcheck entre otras. Algunos fabricantes de productos específicos de seguridad integran también esta funcionalidad dentro de sus herramientas de detección de intrusos. Este es el caso de RealSecure Server Sensor de ISS, Dragon Host Sensor (Squire) de Enterasys, Intruder Alert de Symantec. También existen productos específicos para comprobación de integridad que soportan múltiples sistemas operativos, este es el caso de Tripwire for Servers de Tripwire, Intact de Pedestal Software y Veracity de Rocksoft.

Esta funcionalidad también ha sido introducida de forma natural dentro de algunos sistemas operativos. Algunos ejemplos son ASET (Automated Security Enhancement Tools) proporcionada con el sistema operativo Solaris, el sistema de verificación de integridad integrado en Windows Millenium y XP (no están disponibles en las versiones de servidor NT, 2000 ó 2003) o las herramientas de gestión de paquetes de las distintas distribuciones de Linux, que proporcionan una base de datos propia de integridad con la información de las aplicaciones instaladas.

En la tabla adjunta se muestran algunas de las herramientas de integridad disponibles "de serie" en según qué sistema operativo. No hay que olvidar, sin embargo, que los controles de integridad deberán ajustarse a las necesidades específicas de la organización y al uso que se dará al sistema final.

Sistema Operativo	Herramientas integradas en el sistema operativo
Debian GNU/Linux Mandrake Linux SuSE Linux Red Hat Linux	Sistema de gestión de paquetes (dpkg ó rpm) La mayoría de las de libre distribución
FreeBSD NetBSD OpenBSD	La mayoría de las de libre distribución (en la colección de ports)
HP-UX	Product Description File cksum
Solaris	ASET (Automated Security Enhancement Tools)
Windows (Me, XP)	Windows System Restore

Herramientas de comprobación de integridad ofrecidas por distintos sistemas operativos

La seguridad y fiabilidad de un sistema informativo se consigue en gran medida por una serie de factores, que hay que tener muy en cuenta a la hora de la instalación y administración del sistema y de ello depende que dicho sistema sea más o menos seguro. Dentro de los distintos métodos que se pueden utilizar para conseguir este fin está, sin lugar a dudas, el control de la integridad. Se trata de uno de los más fiables para verificar si un sistema se ha visto comprometido o no. Es conveniente, por tanto, que dentro de los controles de la política de seguridad el control de la integridad esté muy presente. ❑