Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Instalando y configurando Tripwire en debian (21203 lectures)

Per **Elídier Moya R**, ***lillo*** (http://emoya.freeshell.org)

Creado el 20/08/2004 16:34 modificado el 20/08/2004 16:34

Este programa nos ayuda a determinar cuando la seguridad de nuestro equipo ha sido comprometida. Nos informará cuando todas las otras medidas de seguridad han fallado. En la Web es posible encontrar información acerca de su instalación en Red Hat y otros sabores, pero en Debian no encontré nada y tuve que hacerlo todo con el man. Lo que en realidad no resultó tan rápido como yo desearía. Así que aquí va.

Pura Vida! y espero que sea de ayuda

Tripwire

¿Qué hace?

Cuando alguien logra ingresar en nuestro sistema no deseará perder la oportunidad de seguir utilizandolo, por lo que probablemente instalará algo llamado rootkit. Estos rootkit, vistos de una manera muy sencilla, son un conjunto de archivos destinados a reemplazar programas del sistema, creando versiones modificadas para que el administrador no descubra la presencia de procesos extraños, o logs de acceso de usuarios desconocidos.
Por ejemplo, instalan un programa en lugar del pstree original, de modo que cuando se ejecute pstree, no se mostrarán todos los procesos que se están ejecutando. Como puede verse si el administrador no puede confiar en su propio sistema, será muy difícil determinar si este ha sido comprometido.

Instalación y configuración

El primer paso es encontrar y descargar el programa de Internet (si estas usando sarge puedes hacer un sencillo apt-get), seguidamente dpkg -i tripwire.2.3.1.2-0, para instalarlo.

Aquí comienza lo interesante, toda la documentación que puede encontrar me dice que utilice el script install.sh, el cual no encontré por ninguna parte en mi debian. Por lo que el primer paso que realice fue **generar una llave**, el comando utilizado fue

twadmin -m G -L /etc/tripwire/site.key (*Importante***:** Cuidado con las mayúsculas y minúsculas en los parámetros)

Este pide una contraseña (Utilizar una contraseña de verdad, osea que tenga minúsculas, mayúsculas, números y letras)

Seguidamente es necesario **crear un archivo de configuración**. Este se creará basado en el archivo de texto /etc/tripwire/twcfg.txt el cual debemos editar para ajustar a nuestras necesidades. (Yo no tuve que cambiar nada aquí). El comando utilizado para crear el archivo de configuración es:

twadmin -m F -S /etc/tripwire/site.key -c /etc/tripwire/tw.cfg /etc/tripwire/twcfg.txt

Ahora es necesario **crear un archivo llamado nombre_de_mi_host-local.key**, este es idéntico al archivo site.key que creamos antes, por lo que cp site.key nombre_de_mi_host-local.key será suficiente.

El siguiente paso es crear un archivo de políticas, este se creará basado en el archivo /etc/tripwire/twpol.txt (tampoco tuve que modificar nada en este archivo de texto). El comando para generar el archivo de políticas es:

twadmin -m P /etc/tripwire/twpol.txt

Crear la base de datos

Para crear la base de datos (con la información que Tripwire debe monitorear) se utiliza el comando

tripwire -m i 2> /tmp/mensajes

Esta forma de ejecución la encontré aquí [1](1), es un completo tutorial, solamente que es para Red Hat. En él se explica que el comando anterior creará el archivo /tmp/mensajes, donde aparecerá una lista de los archivos que no se encontraron al intentar crear la base de datos.

La duración de este paso dependerá de la cantidad de archivos que desee monitorear, si utilizó las archivos tal y como se instalarón deberá tener paciencia ya que la ejecución tardará. Al finalizar este paso usted verá un nuevo archivo llamado /var/lib/tripwire/nombre_de_mi_host.twd

Verificar la integridad

Cuando deseemos verificar la integridad de nuestro sistema basta con ejecutar

tripwire -m c

y al final veremos un lindo reporte que nos indica si alguno de nuestros archivos ha cambiado desde la creación de la base de datos.

Importante:

Puede que usted desee notificación por correo electrónico. Eso esta bien documentado en el link que mencione antes. [1](1)

[1] http://www.marqueze.net/LuCAS/Tutoriales/GUIA_TRIPWIRE/guia_tripwire.html(1)

Lista de enlaces de este artículo:

1. http://www.marqueze.net/LuCAS/Tutoriales/GUIA_TRIPWIRE/guia_tripwire.html

---

E-mail del autor: emoya _ARROBA_ costarricense.cr