Detección de ataques y respuesta automatizada

OSSEC

Cómo monitorizar y bloquear ataques sin mover un dedo.

POR KURT SEIFRIED

Una de las primeras cosas que se aprenden en seguridad es lo concerniente a los registros [1]. Sin registros, difícilmente se podrá reconstruir lo que pasó antes de romperse algo. La segunda cosa que hay que aprender es que hay que centralizarlos; es el único modo de tener una perspectiva completa y de asegurarse que un atacante no pueda simplemente eliminar los registros de una máquina comprometida, dejándonos sin nada con lo que trabajar. Pero ninguna de estas cosas nos advertirá sobre la irrupción de un atacante, ni tampoco impedirán su entrada. Simplemente, habrá algo que analizar en caso de que se nos cuelen. Entonces, hace falta alguien que esté pendiente, ¿verdad? Bueno, alguien o algún software bien despabilado.

¿No sería genial que pudiésemos monitorizar los archivos de registro críticos (como los de correo o web) y disponer de algo preparado para responder a los potenciales ataques, notificándonoslo, e incluso, de así quererlo, bloqueando el acceso al atacante?. Daniel B. Cid es el jefe de desarrollo del proyecto OSSEC, un esfuerzo por crear un sistema de código abierto de detección de intrusiones basado en hosts [2]. OSSEC hace uso del típico método servidor/cliente: Se instala el software agente en cada sistema a monitorizar, mientras que un servidor central recopila todos los datos y envía alertas. Además, el proyecto OSSEC ha liberado una interfaz web. Aún así, sólo sirve para reportar. Por desgracia, no es posible usarlo para configurar el sistema.

Instalación de OSSEC

Al instalar OSSEC hay tres opciones posibles. La opción de servidor hace que se monitorice a sí mismo y recopile alertas de otros sistemas. La correspondiente al agente simplemente monitoriza los eventos locales y envía cualquier cosa interesante al servidor. La opción local ejecuta la monitorización en forma local y es capaz de enviar emails, pero no atiende a agentes remotos (por lo que resulta la opción adecuada para alguien que tenga un solo servidor o sólo quiera probar el software). Basta con descargar el paquete con OSSEC (*ossec-hids-2.0.tar.gz*), descomprimirlo en cualquier directorio e instalarlo:

```
# wget http://www.ossec.net/➥
files/ossec-hids-2.0.tar.gz
# tar -zxf ossec-hids-2.0.tar.gz
# cd ossec-hids-2.0
# ./install.sh
```

Luego, simplemente elegimos el idioma, el tipo de servidor y si queremos o no ejecutar el demonio de comprobación de integridad, habilitar la respuesta activa y habilitar el cortafuegos para bloquear ataques. Si se está configurando el sistema como agente, también hay que hacer que apunte al servidor y pegar la clave de agente. La clave de agente es una cadena de caracteres larga que se usa para asegurar las comunicaciones entre un agente y el servidor, previniendo la inyección de mensajes y cosas por el estilo. ¿Por qué es esencial evitar que lleguen al servidor mensajes manipulados?

Ojito

Si un atacante consiguiese suplantar o falsificar ataques y, por este motivo, el sistema estuviese habilitado para bloquear direcciones IP, el atacante podría bloquear fácilmente sistemas legítimos y dejar fuera a usuarios. En el peor de los escenarios, si todas las cuentas estuviesen bloqueadas tendríamos que buscar una forma de entrar en nuestro propio sistema, motivo por el cual la mayoría de los sistemas HIDS y NIDS soportan las listas blancas (ver el cuadro *HIDS vs NIDS*). Un administrador puede simplemente crear un listado de máquinas y redes críticas. Claro está que determinar qué máquinas son críticas dependerá de cada instalación en particular (DNS, email, servidores de archivos, servidores de autenticación, encaminadores, etc). En OSSEC, las listas blancas se especifican en el archivo *ossec.conf* (que de forma predeterminada se encuentra bajo */var/ossec/etc/*), pudiéndose especificar tanto máquinas individuales como redes:

```
<global>
 <white_list>127.0.0.1➥
 </white_list>
 <white_list>1.2.3.4➥
 </white_list>
 <white_list>10.0.0.0/8➥
 </white_list>
 <white_list>192.168.0.0/16➥
 </white_list>
</global>
```

Ejecución de OSSEC

El programa OSSEC incluye su propio programa de control llamado *ossec-control*.

Además, al intalarse en Red Hat Linux o en CentOS, se añade un juego de scripts *rc.d/init*, permitiendo el control de los servicios de OSSEC a través de la utilidad estándar *chkconfig*. Durante el tiempo en que OSSEC se encuentre en ejecución, se pueden ver una serie de programas ejecutándose.

Los procesos encargados de la monitorización se han de ejecutar generalmente como root:

```
USER   PID    COMMAND
ossecm 17381 ➥
/var/ossec/bin/ossec-maild
root   17385 ➥
/var/ossec/bin/ossec-execd
ossec  17389 ➥
/var/ossec/bin/ossec-analysisd
root   17393 ➥
/var/ossec/bin/➥
ossec-logcollector
root   17405 ➥
/var/ossec/bin/ossec-syscheckd
ossec  17409 ➥
/var/ossec/bin/ossec-monitord
```

El Agente

Una vez se encuentre el servidor en ejecución, llega el momento de hacer que el resto del grupo le envíe sus reportes. Sólo habrá que instalar el software de OSSEC en cualesquiera máquinas que se deseen monitorizar, escogiendo, claro está, la opción de instalación de agente.

Durante la instalación se nos pide la dirección IP del servidor, así como una serie de opciones estándar relativas a las opciones de monitorización que se aplicarán. Al terminar, se habrá de crear e importar la clave de agente a través del programa *manage_agents*. En el servidor sólo hay que añadir el agente.

Luego, para añadir un agente en particular, hay que extraer su clave, cortarla y pegarla (lo mejor es hacerlo mediante acceso remoto a través de SSH). Simplemente se ejecuta *manage_agents* en el agente y se importa la clave. El proceso es similar bajo Windows, aunque la opción predeterminada es la de la interfaz gráfica para facilitar las cosas (por suerte, están disponibles las versiones de línea de comandos para todos los programas disponibles, lo que permite una gestión remota basada en scripting desde la línea de comandos).

De forma predeterminada, OSSEC monitoriza todos los archivos de los directorios */etc*, */bin*, */sbin*, */usr/bin* y */usr/sbin* (esencialmente, las entrañas de cualquier sistema), así como un gran número de archivos de registro de demonios (*named*, *smbd*, *mysql*, *telnetd*, etc.).

Los directorios que se monitorizarán, al igual que los nuevos juegos de reglas para los servicios de monitorización, se pueden configurar editando el archivo *ossec.conf*, que presenta un formato al estilo de XML bastante autoexplicativo.

La Interfaz Web

Ahora que ya está OSSEC correctamente instalado y protegiendo la red, ¿qué hacemos? Una increíble funcionalidad de OSSEC es la relativa a los reportes. Por ejemplo, es posible generar reportes en texto a partir de la actividad máxima de una o varias direcciones IP, los nombres usados en los intentos de login fracasados, etc.

La interfaz web de usuario de OSSEC permite realizar peticiones específicas, aunque por desgracia no permite la configuración de los servidores o de los agentes (para eso hay que recurrir a la línea de comandos).

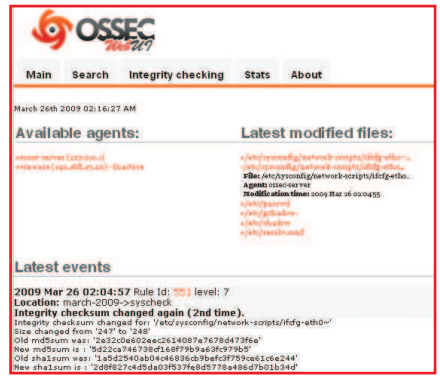

Figura 1: La pestaña Main de la interfaz web de OSSEC muestra información sobre eventos y sobre los últimos archivos modificados.

Además, la WebUI de OSSEC permite conocer el estado del servidor y de los agentes de un vistazo (Figura 1).

Tripwire

No se nos quedará en el tintero Tripwire [3]. Tripwire es el padre de todos los HIDS, monitorizando y reportando cambios en los archivos de sistemas Unix (ahora también de Windows), encaminadores y otros dispositivos.

Tripwire aún se encuentra disponible como paquete de fuentes abiertas; aunque no se ha actualizado en varios años, se podría aseverar que se trata de un proyecto terminado.

Conclusiones

Uno de los mayores problemas de la seguridad es la cantidad de esfuerzo que se requiere en la instalación y mantenimiento permanente. OSSEC proporciona un grado de seguridad y protección activa con un coste mínimo en instalación y con poco mantenimiento. Carece de algunas funcionalidades que estarían realmente bien (como indicar qué ha cambiado en un archivo, en vez de decir solamente que el archivo ha cambiado), así como otras para facilitar su uso (como gestión de cambios y configuraciones masivas), pero dichas carencias se ven compensadas por la facilidad de instalación y gestión. ■

HIDS vs NIDS

Los sistemas de detección de intrusiones basados en host (HIDS) se definen generalmente como aplicaciones que se ejecutan en sistemas específicos y que monitorizan archivos de registro locales, actividad en la red y otros elementos útiles para la detección de comportamientos hostiles. La ventaja de los HIDS es que cuentan con un acceso más profundo al sistema y relacionan entre sí los eventos locales fácilmente (por ejemplo, un error en una aplicación web seguido de un nuevo usuario añadido al sistema). La desventaja, que se ha de instalar el software en cada una de las máquinas que se desea proteger y se han de administrar muchos puntos finales.
Los sistemas de detección de intrusiones por red (NIDS) suelen constar de uno o más sensores de red ubicados en puntos de paso obligado (como los cortafuegos), o enganchados a switches configurados para redirigir al sensor todo el tráfico. La ventaja de los NIDS es que es posible cubrir con ellos grandes porciones de una red con una cantidad mínima de sensores. La desventaja es que los ataques internos pueden pasarnos desapercibidos cuando no atraviesan las partes monitorizadas de la red, privándonos de la oportunidad de analizar los sistemas en mayor profundidad.

RECURSOS

[1] "Inmersión" por Heike Jurzik, Linux Magazine, Número 40, *http://www.linux-magazine.es/issue/40/085-086_LdeCLogsLM40.pdf*

[2] OSSEC: *http://www.ossec.net/*

[3] Tripwire: *http://sourceforge.net/projects/tripwire/*