Seguridad en Sistemas Informáticos (SSI)

Laboratorio: OSSEC

Contenido

Introducción

En esta práctica se introduce la herramienta OSSEC, un detector de intrusos basado en nodo (HIDS, Host-based Intrusion Detection System) que lleva a cabo las siguientes funciones:

* análisis de registros
* comprobación de integridad
* detección de rootkits
* alertas basadas en secuencias temporales
* respuesta activa

OSSSEC puede trabajar de dos formas:

* En modo local, en el que se instala en cada nodo que tiene que ser protegido. Entonces, en cada nodo se llevan a cabo las todas las funciones citadas anteriormente.
* En modo servidor/agente, donde hay una única máquina (el servidor) que realiza el análisis y la correlación de eventos. Las demás envían los eventos al servidor, de forma que el conjunto es mucho más sencillo de configurar y administrar.

Objetivos

* Introducir los sistemas de detección de intrusos basados en nodos (HIDS).
* Introducir OSSEC como caso de estudio de los HIDSs.
* Comprobar la detección y reacción automática frente a un ataque por fuerza bruta al servidor de SSH.

Realización de la práctica

Para plantear un caso más realista, se utilizará OSSEC en modo servidor/agente, utilizando la siguiente infraestructura:

* la máquina virtual VMWare (base.example.net actuará como servidor)
* las máquinas exta y extb actuarán como agentes
* la máquina extf actuará como atacante

Durante la práctica se instalará OSSEC en las diferentes máquinas virtuales y después se simulará un ataque por fuerza bruta sobre el servidor SSH de extb, comprobando que el ataque es detectado y que se toman medidas automáticas para repelerlo.

Puesta en marcha del sistema

* Arrancar la máquina virtual VMWare de la asignatura (base.example.net).
* Arrancar las máquinas virtuales UML siguientes: exta, extb y extf.

Instalación y configuración de OSSEC en el servidor

Trabajando como el administrador de "base.example.net", llevar a cabo los siguientes pasos:

Obtener una copia de OSSEC:

```
base:~# wget http://www.ossec.net/files/ossec-hids-latest.tar.gz
base:~# wget http://www.ossec.net/files/ossec-hids-latest_sum.txt
```

Comprobar la integridad del programa:

```
base:~# cat ossec-hids-latest_sum.txt
MD5 (ossec-hids-latest.tar.gz) = XXXXXXX
SHA1 (ossec-hids-latest.tar.gz) = YYYYYYYY
base:~# md5 ossec-hids-latest.tar.gz
MD5 (ossec-hids-latest.tar.gz) = XXXXXXX
base:~# sha1 ossec-hids-latest.tar.gz
SHA1 (ossec-hids-latest.tar.gz) = YYYYYYYY
```

Instalar y configurar OSSEC en modo servidor:

```
base:~# tar -zxf ossec-hids-*.tar.gz
base:~# cd ossec-hids-*
```

base:~# ./install.sh

Seleccionar la instalación en modo servidor, utilizando las opciones por defecto durante la ejecución de ./install.h, pero teniendo cuidado de proporcionar una dirección de correo válida para recibir las notificaciones (sugerencia: usar "unp@base.example.net").

Detener el cortafuegos de "base.example.net":

base:~# rcSuSEfirewall2 stop
(En realidad es suficiente con abrir el puerto 1514 de UDP).

Instalación y configuración de los agentes

Repetir el siguiente procedimiento para exta y extb.

Obtener una copia de OSSEC:

scp base:ossec-hids-*.tar.gz .

Instalar y configurar OSSEC en modo agente:

tar -zxf ossec-hids-*.tar.gz
cd ossec-hids-*
./install.sh

Seleccionar la instalación en modo agente, proporcionando la dirección IP del servidor (10.5.0.1).

Gestión de los agentes

La comunicación entre el servidor y los agentes es encriptada y autentificada. Por este motivo, para cada agente es necesario crear una clave de autentificación en el servidor, exportarla, e importarla en el cliente.

A continuación se describe el mecanismo para exta. (Este mismo mecanismo debe ser repetido posetiormente para extb teniendo cuidado de usar el identificador, nombre y dirección IP adecuados).

1. Dar de alta a exta en el servidor:

```
base:~# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v1.1 Agent manager.       *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to main menu).
  Please provide the following:
    * A name for the new agent: exta
    * The IP Address for the new agent: 10.5.0.10
    * An ID for the new agent[001]:
Agent information:
    ID:001
    Name:exta
```

IP Address:10.5.0.10

Confirm adding it?(y/n): y
Added.

2.Generar y exportar una clave de autentificación para exta:

base:~# /var/ossec/bin/manage_agents

```
****************************************
* OSSEC HIDS v1.1 Agent manager.       *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your actions: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: exta, IP: 10.5.0.10
Provide the ID of the agent you want to extract the key: 001

Agent key information for '001' is:
CDAxIGxpbnX4MSAxOTIuMTY4LjAuMzIgOWM5MENlYzNXXX
YYYZZZZZ==

** Press ENTER to return to the main menu.
```

3.Importar la clave de autentificación en exta:

exta:~# /var/ossec/bin/manage_agents

```
****************************************
* OSSEC HIDS v1.1 Agent manager.       *
```

```
* The following options are available: *
****************************************
   (I)mport key for the server (I).
   (Q)uit.
   Choose your actions: I or Q: i

* Provide the Key generated from the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here:
CDAxIGxpbnX4MSAxOTIuMTY4LjAuMzIgOWM5MENlYzNXXXYY
YZZZZZ==

Agent information:
   ID:001
   Name:exta
   IP Address:10.5.0.10

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.
```

Tal y como sugiere el propio programa, la forma más sencilla de transportar la clave es utilizando la opción y de copiar y pegar con el ratón.

Puesta en marcha de OSSEC

Arrancar el servidor y los agentes ejecutando /var/ossec/bin/ossec-control start en cada uno de los nodos.

Realización del ataque

Desde extf simular un ataque de fuerza bruta contra el servidor SSH de extb:

```
extf:~# ssh x@extb
x@extb's password:
Permission denied, please try again.
x@extb's password:
Permission denied, please try again.
x@extb's password:
Permission denied (publickey,password).

extf:~# ssh y@extb
(igual que antes)

extf:~# ssh z@extb
(idem)

extf:~# ssh a@extb
(no responde)
```

Detección y respuesta automática

Al detectar el ataque en base al registro generado por el servidor de SSH en extb, OSSEC debería realizar las siguientes acciones:

* Enviar un correo electrónico (a la dirección especificada al instalar el servidor) alertando del hecho.
* Añadir una entrada a /etc/hosts.deny en extb denegando el acceso a sshd desde extf.
* Añadir sendas reglas a la configuración de iptables de extb impidiendo cualquier tipo de tráfico entre extb y extf.

Para finalizar la práctica se pide:

* Comprobar que efectivamente se han producido las tres acciones recién descritas.
* Comprobando la configuración de OSSEC, responder a las siguientes preguntas:
    1. ¿Cuánto tiempo dura la modificación del fichero hosts.deny?
    2. ¿Cuánto tiempo dura el cambio en la configuración de iptables?
    3. Durante la prohibición, ¿podría conectarse extd a extb?
    4. Si el usuario carlos falla cuatro veces al intentar conectarse a extb, ¿también se activarían las medidas anti-intrusos?
* Subir a aula virtual, como respuesta a la actividad "OSSEC" los siguientes documentos:
    - o copia del correo electrónico de alerta
    - o copia del fichero /etc/hosts.deny de extb
    - o copia de la configuración de iptables en extb (sugerencia, usar iptables -L)
    - o respuestas a las preguntas