Herramienta de detección de instrucciones (Aide, Samhain, Snort)

David Berrocal Macías

Departamento de Informática y Automática, Universidad de Salamanca.

Plaza de la Merced, s/n, 37008, Salamanca, España

dabm@usal.es

Resumen. Durante los últimos años, los ataques cibernéticos han sufrido un importante incremento, llegando a generar pérdidas millonarias a las organizaciones afectadas. Una buena alternativa para mejorar la seguridad de nuestros datos consiste en la instalación de IDS o Sistemas de Detección de Intrusos, cuya principal función es la de detectar accesos no deseados a nuestra red o comportamientos anómalos en el interior de esta. En este proyecto se va a estudiar el funcionamiento de varios IDS: Snort, Aide y Samhain. Para analizar el tráfico y realizar representaciones graficas que ayuden a su monitoreo.

Palabras clave: IDS, Snort, Samhain, Aide

1. Introducción

En la actualidad y por lo general las propiedades de gran valor necesitan ser protegidas tanto de posibles robos como de la destrucción de estas, es por esto por lo que se usan sistemas de alarma y monitoreo para aviar en tiempo real a los dueños o a la policía de estas situaciones.

Los sistemas informáticos deberían protegerse de igual forma, la información es hoy en día muy valiosa, es por esto por lo que se instalan sistemas de detección de intrusiones o IDS: Intrusion Detection System. Un IDS es un programa de detección de accesos no autorizados a un host o a una red o un sistema de ficheros.

El funcionamiento de estas herramientas se basa en el análisis del tráfico de red o el sistema de ficheros, el cual se compara con una base de firmas de ataques conocidos o comportamientos sospechosos, como puede ser el escaneo de puertos y paquetes malformados o accesos a ficheros protegidos.

2. Antecedentes

La Información es considerada el activo más importante de las empresas. Si la información de una organización llegara a desaparecer o cayera en manos de la competencia, tendría un impacto crítico para la organización y en algunos casos a la economía de un país. Por esta razón, mantenerla a salvo es un objetivo fundamental. Una de las medidas preventivas sería la instalación de sistemas de detección de intrusiones, considerando una intrusión como el conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.

Los dos grandes sistemas de detección de intrusiones son los IDS (Intrusion Detection System) y los IPS (Intrusion Prevention System). Nos centraremos en los sistemas IDS.
Un sistema de detección de intrusos o IDS es un mecanismo de seguridad que lleva a cabo el análisis automático de parámetros de un entorno con el propósito de detectar intrusiones. Cuando se identifica una condición anómala, el IDS emite una alerta con datos relacionados de la misma.

3. Sistemas de Detección de Intrusiones (IDS)

Analizaremos principalmente tres sistemas IDS: AIDE, Samhain y Snort.

El funcionamiento de la última herramienta de detección de intrusos se basa en el análisis del tráfico de red, el cual al entrar al analizador se compara con firmas de ataques ya conocidos, o comportamientos sospechosos, como el escaneo de puertos, paquetes malformados o anómalos, incumplimiento de políticas de seguridad.
Estos IDS no sólo se encargan de analizar qué tipo de tráfico es, sino también del contenido de los paquetes y su comportamiento. Esta última característica permitiría detectar ataques nuevos contra los sistemas.

Aunque no hace falta tener un cortafuegos para la utilización de un IDS, es altamente recomendado y grandes empresas adoptan estas medidas de protección a la vez.

Mientras que AIDE y Samhain se basa en el monitoreo de sistemas de ficheros para detectar cambios en permisos, ficheros o actitudes sospechosas de intentos de lectura/escritura.

3.1 Tipos de IDS

Existen diferentes tipos de IDS, forma en la que detectan las intrusiones y según su reacción al detectar un posible ataque:

- Clasificación según la técnica de análisis:
  - Detección de usos anómalos: este tipo de detección se apoya en comprender cuál es el tráfico común de la red, para generar alertas cuando detecte tráfico fuera de lo normal.
  - Detección de usos indebidos: en este tipo de detección, no se conoce lo que es normal en un sistema, sino que se conocen los ataques hasta la fecha, de tal manera que cuando se detecte un ataque conocido se creará una alerta. La aproximación más habitual es la búsqueda de patrones, cada intrusión tiene un patrón o firma asociado a ella, que serán interpretados por el IDS.

- Los IDS también se pueden clasificar según su reacción ante un posible ataque:

  - Respuestas Pasivas: se detecta un posible ataque o violación de la seguridad, se registra la información detectada del ataque y se genera una alerta de la intrusión.

  - Respuestas Reactivas: el IDS es capaz de iniciar una respuesta automática ante una actividad, por ejemplo, si se detecta un acceso de un usuario no autorizado, es capaz de sacar a dicho usuario del sistema, o si se detectase un ataque de criticidad alta desde una IP hostil, sería capaz de configurar el cortafuegos filtrando dicha IP.

3.2 Snort

Snort”1 un *sniffer* de paquetes y un sistema de detección de intrusos basado en red, gratuito, bajo licencia GPL y puede ser instalado tanto en sistemas operativos Windows como en sistemas UNIX/Linux.
Implementa un motor de detección de ataques el cual permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Existen herramientas complementarias a Snort que hacen que este IDS sea un sistema muy completo y fácil de administrar. Como, por ejemplo, herramientas que almacenan las alertas detectadas por Snort en una base de datos (Barnyard2) y otras que recogen de esta base de datos las alertas y las muestran en una interfaz gráfica (BASE).

Snort implementa un lenguaje de creación de reglas flexible, potente y sencillo, pudiendo crear todas las alertas que se requiera. Un usuario puede crear una regla y compartirla a través de Internet para que todos los demás usuarios se puedan beneficiar de esta firma o patrón de detección.

Existen grandes comunidades”2 las cuales nos ofrecen gran cantidad de reglas de ataques y conexiones sospechosas que podemos incluir en nuestro IDS de manera gratuita y de pago.

Snort puede funcionar en los siguientes tres modos:

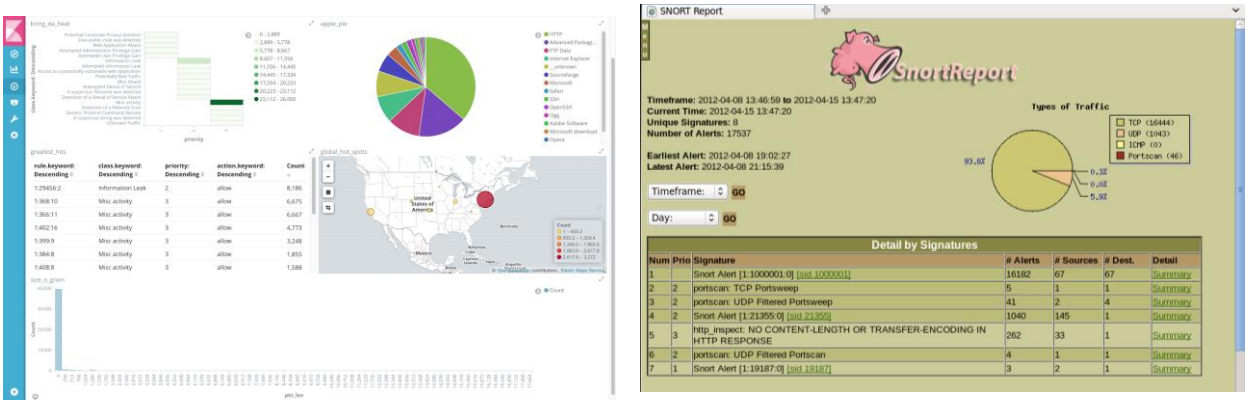
- Modo Sniffer: se captura el tráfico en tiempo real de la red configurada en el archivo de configuración de Snort y se imprime por pantalla.

- Modo registro de paquetes: se guardan los paquetes de la red configurada en el archivo de configuración de Snort, pudiendo volver a reproducir el tráfico almacenado en los ficheros posteriormente.

- Modo NIDS: se comparan las tramas de todos los paquetes con el conjunto de reglas o patrones que se tengan configurados.

Una vez instalado, se deberán agregar los conjuntos de reglas que se quieran utilizar para detectar las actividades sospechosas que afecten en la red.
Cuantas más reglas se añadan, más se sobrecarga el programa, pudiendo llegar a tasas de pérdida de paquetes no analizados muy elevadas, con lo que habrá ataques que el IDS no detecte.

De los datos en bruto que nos otorga Snort podemos crear herramientas visuales personalizadas para mejorar la representación y que sea más fácil monitorear los sistemas, un ejemplo de estas interfaces:



Interfases gráficas sobre Snort.

Ejemplo uno: regla en Snort:
En el fichero de reglas locales: /etc/snort/rules/local.rules
Añadimos, por ejemplo:

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Alguien ha intentado acceder a bhal/fichero"; content:"/blah/fichero";)

Se generará una alerta cada vez que alguien desde una IP externa, desde cualquier puerto, realice una petición al puerto 80 de una IP interna.

La segunda parte de la regla indica que para que se active, en la petición debe acceder a "/blah/fichero".

Ejemplo dos, analizando entrada FTP a una maquina local:

Configuramos la regla

- sudo gedit /etc/snort/rules/local.rules
- alert tcp 192.168.x.x any -> $HOME_NET 21 (msg:"FTP connection attempt";)

Iniciamos snort
- sudo snort -A console -q -c /etc/snort/snort.conf -i eht0 -K ascii

Realizamos el ataque:

```
root@attackserver:~# ftp 192.168.132.130
ftp: connect: Connection refused
ftp>
```

En la maquina local veremos la alerta:

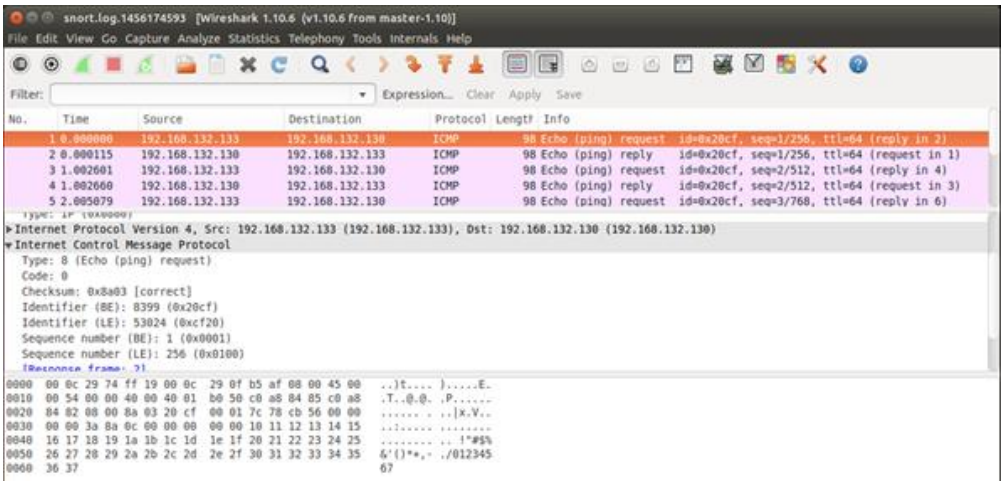
```
stu@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i eth0 -K ascii
02/22-14:09:47.453755  [**] [1:1000002:1] FTP connection attempt [**] [Priority:
 0] {TCP} 192.168.132.133:45562 -> 192.168.132.130:21
```

Analizamos las tramas involucradas:

Si analizamos los ficheros generados en /var/log/snort, por cada alerta genera un log con un identificador

```
stu@ubuntu:~$ ls /var/log/snort/
192.168.132.133  archived_logs  snort.log.1456174593
stu@ubuntu:~$
```

Si abrimos el snort.log.XXX en wireshark por ejemplo, podremos ver todos las paquetes implicados:



3.3 AIDE (Advanced Intrusion Detection Environment)

AIDE”3 (Advanced Intrusion Detection Environment) es una herramienta de detección de intrusos para verificar la integridad de archivos y directorios. El funcionamiento se basa en crear una base de datos con información importante de los archivos y directorios (por ejemplo: nombre, tamaño, fecha de modificación, permisos y un hash del contenido) y luego comprobar periódicamente contra esta información de referencia para verificar que no se hayan producido cambios inesperados.

Lo ideal es generar la base de datos de AIDE inmediatamente luego de instalar un sistema y a partir de ahí monitorear los cambios que se producen.

El archivo de configuración predeterminado se puede encontrar en /etc/aide.conf. Este archivo presenta varios ejemplos de reglas de protección (por ejemplo, FIPSR, NORMAL, DIR, DATAONLY), cada una de las cuales va seguida de un signo igual y una lista de atributos de archivo para verificar, o cualquier regla predefinida (delimitada por un signo más). También puede definir cualquier regla personalizada utilizando este formato.

/etc/aide.conf

```
FIPSR = p+i+n+u+g+s+m+c+acl+selinux+xattrs+sha256
NORMAL = FIPSR+sha512
# For directories, don't bother doing hashes
DIR = p+i+n+u+g+acl+selinux+xattrs
# Some files get updated automatically, so the inode/ctime/mtime change
# but we want to know when the data inside them changes
DATAONLY =  p+n+u+g+s+acl+selinux+xattrs+sha256
# Custom rule:
SCRIPTS = p+n+u+g+s+acl+selinux+md5
```

Lo anterior significa que la regla NORMAL comprobará las inconsistencias en los siguientes atributos: permisos (p), inodo (i), número de enlaces (n), usuario (u), grupo (g), tamaño (s), mtime (m), ctime (c), ACL (acl), SELinux (selinux), xattrs (xattr), sumas de comprobación SHA256 / SHA512 (sha256 y sha512).

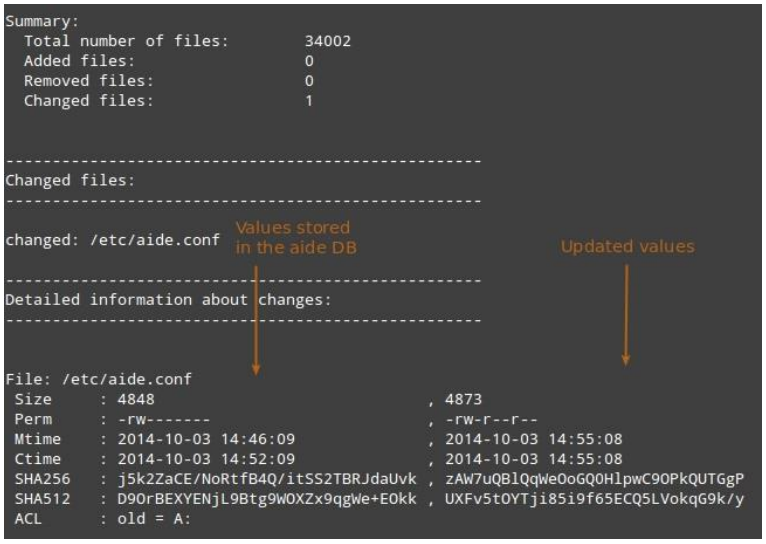
Ejemplo sencillo de uso: tras instalar AIDE por apt, debemos inicializar su base de datos con: #aideinit

Por defecto AIDE instala el cron /etc/cron.daily/aide. Este script se ejecuta diariamente e informa por correo electrónico los cambios que encuentre en el sistema de archivos. La cuenta de correo que utiliza como destino se configura en el archivo /etc/default/aide en la variable MAILTO.

MAILTO=dabm@usal.es

Adicionalmente, para que se actualice la base de datos a diario:
en el archivo /etc/default/aide en la variable COPYNEWDB a yes.
Esto creara una nueva db diaria.

COPYNEWDB=yes



Salida por pantalla tras analizar el sistema de ficheros con Aide

De esta forma podemos saber con exactitud qué cambios ocurren en nuestro sistema, y además seremos notificados por correo.

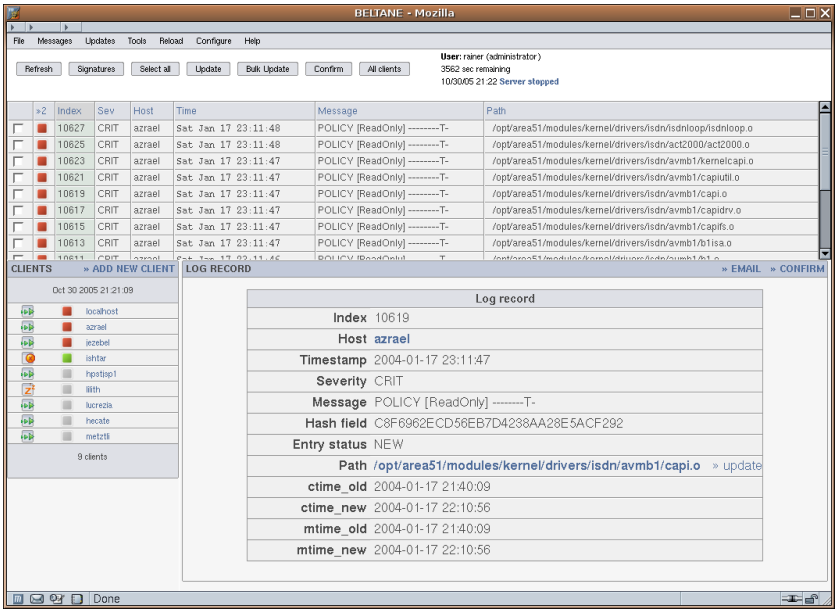
4. Samhain

Samhain”4 es una aplicación HIDS (Sistema de detección de intrusos en un Host) de código abierto especialmente diseñada para monitorear la integridad de los archivos del sistema. Samhain se puede implementar de dos maneras diferentes, ya sea en modo independiente (local) o en modo cliente/servidor, pose capacidades de ejecutarse de forma totalmente escondida usando esteganografía.

La función más importante de Samhain HIDS es monitorear la integridad de los archivos, auditorías SUID y SGUI (permisos de acceso), monitorear las configuraciones de montaje, los log-in y log-out, realizar una verificación de integridad del Kernel para detectar posibles Rootkits y, finalmente, puede monitorear la integridad de la tabla syscall”5.

Samhain tiene diferentes tipos de opciones de configuración y cada una de estas opciones se puede usar por separado para un propósito específico, pero la opción de monitoreo de integridad de archivos se instala de manera predeterminada. A diferencia de otras aplicaciones de HIDS, ciertas opciones pueden personalizarse para tareas específicas.

La consola Beltane”6 basada en la web, disponible como paquete separado, permite monitorear la actividad del servidor y del cliente, ver los informes de los clientes y actualizar las bases de datos de referencia.



Consola web Beltane para Samhain

Ejemplo sencillo de Samhain en local:

Tras instalar y configurar Samhain, debemos iniciar su base de datos para que empiece a funcionar, con: # samhain –t init
En el momento en que Samhain termine de crear la base de datos, la guardará en el directorio (/var/lib/samhain/).

samhain –t check –p warn –foreground

Tras este comando comienza a escanear todo el sistema en busca de amenazas o actividad sospechosa. Es importante tener en cuenta que Samhain puede ejecutarse como un demonio en proceso en segundo plano, por lo tanto, se debe usar "--foreground" para que podamos ver las alertas de error.

Referencias

1. Proyecto Snort: https://www.snort.org/
2. Descarga de patrones para Snort (https://www.snort.org/downloads)
3. AIDE https://en.wikipedia.org/wiki/Advanced_Intrusion_Detection_Environment
4. Samhain https://la-samhna.de/samhain/
5. “System calls provide interface between user applications and privileged kernel space and are the primary target for most rootkits. The handler for each system call is stored in a system call table (Wotring, 2005).”.
6. Interfaz beltane para Samhain https://www.la-samhna.de/beltane/