Detección de intrusos en GNU/Linux

David Fernández Vaamonde
david_fv@gpul.org
II Ciclo de conferencias "Seguridad en Internet y Telecomunicaciones"

28 de abril de 2002

Resumen

En esta ponencia se desarrolla el tema de la detección de intrusos, tema importante en el ámbito de la seguridad informática como prevención ante posibles abusos contra nuestros sistemas. También se presentarán algunas de las soluciones más usuales para GNU/Linux todas ellas software libre.

1. ¿ Por que GNU/Linux y software libre?

Cuando tratamos el tema de la seguridad informática, se nos olvida en muchos casos tratar temas de base tan importantes que pueden convertirse frecuentemente en un problema de seguridad en si mismos.

La pregunta surge rápidamente ¿ Podemos implantar cualquier sistema de seguridad en cualquier ordenador ? La respuesta es: NO. Una máquina que pretende dar seguridad a otras o a una red completa, ha de ser una máquina robusta, que soporte bien ciertos fallos y que permita mucha flexibilidad. Por eso mismo he elegido el sistema operativo GNU/Linux[1]

Este sistema operativo destaca por ser muy estable y robusto:

- Tiene unos uptimes muy elevados
- Permite cambiar configuraciones en caliente
- Soporta tolerancia a fallos:
    - Alta disponibilidad

[1]... Que a partir de este momento llamaré Linux por economía lingüistica

    - Sistemas de ficheros con journaling
    - Soporte de RAID
- Es muy flexible por seguir la filosofía UNIX
- Registros y ficheros de log muy completos
- Es software libre.

Es interesante que sea software libre por varias razones importantes para la seguridad informática: en primer lugar, si existe algún problema en la máquina, tengo las fuentes para intentar arreglar el problema si quiero, por otra parte, tengo las fuentes siempre para comprobar que software estoy instalando en mi máquina, asegurándome que no añado a mi sistema nada que yo no considere necesario.

Esta son las razones que me llevan a hablar en esta ponencia de detección de intrusos de programas de software libre que en su mayoría corren en Linux, antes de preocuparnos por los programas que cubrirán nuestra seguridad, hemos de preocuparnos por la seguridad de base del sistema que estamos implantando.

2. ¿ Que es un sistema de detección de intrusos ?

La seguridad en un sistema podríamos clasificarla de dos modos: activa y preventiva. La seguridad activa de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo. Un firewall es un buen ejemplo de seguridad activa, trata de filtrar el acceso a ciertos servicios en determinadas conexiones para evitar el intento de forzamiento desde alguno de ellos.

Por otro lado, la seguridad preventiva es aquella que implantamos en nuestro sistema para que nos informe si en el está teniendo lugar una incidencia de seguridad. No pretende proteger el sistema, pretende alertarnos de que algo extraño esta sucediendo en el. Un buen ejemplo de seguridad preventiva es un sistema de detección de intrusos.

Un sistema de detección de intrusos es aquel que nos permite recabar información de distintas fuentes del sistema en el que se implanta para alertar de un posible intrusión en nuestras redes o máquinas. La alerta puede ser del hecho de que existe un intento de intrusión, como del modo en el que este se está realizando y en algunos casos por parte de quén esta siendo efectuado. Podemos considerar un sistema de detección de intrusos como un *control de auditoría* que nos permitirá tomar decisiones a la hora de realizar una auditoría de seguridad de nuestro sistema.

Un sistema de detección de intrusos surge como una medida preventiva, nunca como una medida para asegurar nuestros sistemas, ayudan al administrador de dicho sistema a permanecer al tanto de cualquier intención aviesa contra el sistema que administra.

3. Tipos de sistemas de detección de intrusos

Llegados a este punto es interesante clasificar de algún modo los distintos sistemas de detección de intrusos.

Una primera clasificación puede ser entre **sistemas en tiempo real** y aquellos que no lo son.

Los sistemas en tiempo real permanecerán constantemente chequeando el sistema buscando alguna señal de un incidente de seguridad e inmediatamente provocarán una alarma. Por contra, los sistemas de detección de intrusos que no son de este tipo se usan generalmente cuando existe la creencia de que estamos ante un incidente de seguridad y se usan para recabar información del tipo y alcance de esta incidencia, generalmente sobre registros o información del sistema.

Una clasificación más rigurosa la podemos realizar según los medios que utilizan los sistemas de detección de intrusos para monitorizar las incidencias. Tenemos según esta clasificación cuatro tipos de sistemas:

- **Basados en el host**. Estos sistemas recaban información del sistema para realizar un analisis de las posibles incidencias pero siempre desde el punto de vista del propio sistema y con sus recursos.
- **Basados en la red**. Sistemas que observan el tráfico de red buscando algún indicio de un ataque conocido. Generalmente un interfaz en modo promíscuo buscando datos sobre una red. (Suelen pertenecer también al tipo de tiempo real).
- **Basados en la aplicación**. Estos recaban datos de una aplicación activa en el sistema (por ejemplo los logs u otra) y buscan evidencias en estos datos. La diferencia con los basados en host es que estos los propios recursos son detectores de intrusos y en el caso de aplicación los datos han de ser filtrados para ser tratados como alarmas.
- **Basados en el objetivo**. Estos monitores se basan en salvaguardar la integridad del objetivo que podría ser cualquier recurso del sistema (por ejemplo el sistema de ficheros).

Ya por último y para terminar esta taxonomía podemos diferenciar los sistemas de detección de intrusos según el tipo de analisis que realiza:

- **Detección de uso inadecuado**. En estos casos el sistema busca un patrón de un ataque bien definido.
- **Detección de alguna anomalía**. Se busca sobre el sistema alguna anomalía que pueda hacer creer que hay un incidente de seguridad, pero que puede no ser provocada por esto.

4. Arquitectura de un sistema de detección de intrusos

Prácticamente todos los sistemas de detección de intrusos tienen ciertas partes bien definidas que pasamos a comentar seguidamente:

- **Fuentes de recogida de datos de aplicaciones**. Punto de recogida de datos para análisis actual o posterior que bien puede ser una red, el sistema o elementos que residen en el propio sistema.
- **Reglas**. Estas reglas en muchos casos son las que caracterizan las violaciones que pueden ser cometidas y contra las que se contrastan los datos obtenidos en el punto anterior.
- **Filtro**. Esta parte se encarga de contrastar las reglas contra los datos obtenidos.
- **Detectores de anomalías**. En los casos de análisis por anomalías son aquellos que detectan eventos extraños en el sistema o los recursos monitorizados.
- **Generador de informes o alarmas**. Una vez que se han procesado los datos contra las reglas por el filtro y si existe alguna situación que haga creer que se ha vulnerado o intentado vulnerar la seguridad del sistema, esta parte del detector de intrusos informa al administrador de este hecho (mediante correo, mensajes a móviles, avisos acústicos, etc...).

En la figura 1 podemos ver gráficamente como se puede diseccionar la arquitectura de un sistema de detección de intrusos.

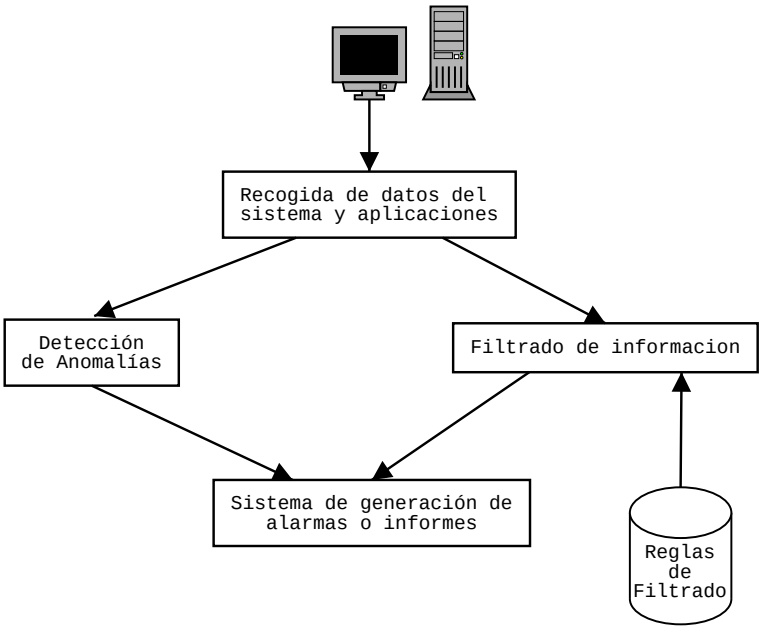

Figura 1: Arquitectura de un sistema de detección de intrusos

5. Sistemas de detección de intrusos bajo GNU/Linux

Bajo GNU/Linux corren una amplio abanico de soluciones para detectar intrusos, desde las más sencillas hasta las más complejas. Podemos decir que un simple *find*, ejecutado buscando cambios aparentes en los ficheros que tienen de *setuid* root en el sistema y comparándolos con otros anteriores, puede ser un sistema de detección de intrusos donde aparecen casi todos sus componentes, véase: recabamos datos del sistema, la regla y el filtrado es inherente al find y a la condición que hemos impuesto sobre el y el sistema de notificación el que nos quiera dar nuestro pequeño script. Esto es fruto de la flexibilidad de un sistema Unix. Sin embargo trataremos aquí algunas de las soluciones específicas diseñadas a tal efecto para servir como sistema de detección de intrusos general en su ámbito concreto.

5.1. Logcheck

La aproximación de logcheck es la de un sistema de detección de intrusos que hace las veces de uno de los mas arduos trabajos del administrador de sistema : el revisar constantemente los ficheros de

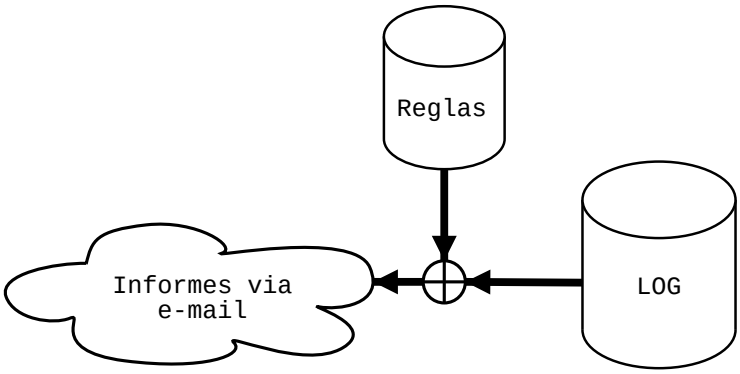

Figura 2: Esquema de funcionamiento de Logcheck

log[2] para detectar alguna anomalía.

Logcheck es lanzado por el *cron* [3] cada cierto tiempo y mediante comparaciones, trata los datos almacenados en los logs contra una serie de reglas (expresadas en términos de expresiones regulares).

Estas reglas presentan patrones definidos que aparecen en los logs de la máquina cuando estas están bajo algún intento de forzamiento de de modo que busca en los registros patrones parecidos.

Un ejemplo de regla de logcheck:

```
login.*: .*LOGIN FAILURE.* FROM .*root
```

En este caso, la regla coincide con todas aquellas líneas donde el subsistema login tenga un fallo cualquiera al intentar hacer login como superusuario.

Este sistema de detección de intrusos, en las categorías dadas anteriormente, a caballo entre las que están basados en el host y las basadas en la aplicación. Esto es debido a que el chequeo que se realiza, se hace sobre los ficheros de log del sistema (por tanto podría ser basada en host), pero sin embargo es la aplicación de log (syslog) quien proporciona los datos.

Logcheck es una herramienta muy flexible y extremadamente configurable, sin embargo es necesario tener buena mano en su configuración sino las alertas tienden a ser elevadisimas.

[2]Ficheros de registros del sistema, donde se muestra la actividad del mismo en cada instante de tiempo

[3]Herramienta de los sistemas unix que permite lanzar tareas a un intervalo definido

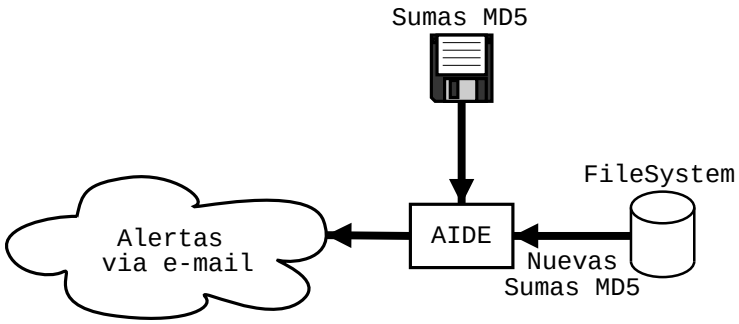

Figura 3: Esquema de funcionamiento de AIDE

5.2. AIDE

El programa AIDE, surge como una iniciativa de clonar un sistema de detección de intrusos muy famoso denominado *Tripwire*, el cual no es software libre. Este sistema se basa en considerar la integridad de los archivos como una de las alarmas de que ha existido una intrusión. De todo el mundo es sabido que una de las acciones más comunes de un intruso en un sistema es garantizar el acceso a este sistema aunque el fallo por el que ha accedido a el sea corregido, para ello, los infractores introducen programas que suplantan a los actuales y que habitualmente tienen un fin añadido (generalmente la obtención de datos del sistema, passwords, implantan puertas traseras, etcétera.)

La aproximación que tanto AIDE como Tripwire adoptan es la de salvaguardar ciertos datos de los sistemas de ficheros de modo que comparando la situación actual de los mismo con la obtenida posteriormente, se pueda saber que ficheros han cambiados. Ambos programas marcan ciertos directorios como `/usr/bin` como aquellos cuyos ficheros no deben ser cambiados. Tras hacer esto, se extraen sumas MD5[4] o de otro tipo y se guardan fuera del sistema (un disquete, una cinta, etcétera).

Si el administrador del sistema, por algún motivo cree que ha podido ser objetivo de una intrusión, recupera las sumas originales, el programa realiza las sumas actuales y las compara, si en algún fichero las sumas no coinciden se da una alarma ya que puede significar que alguien alteró el fichero con intenciones aviesas. Con este tipo de sistemas no solo podemos obtener la alarma de que alguno de nuestros ficheros ha cambiado sino que también aislaremos el fichero en cuestión.

[4] Algoritmo que realiza ciertas operaciones sobre datos para dar un resultado que únicamente será igual si se realizan dichas operaciones sobre los mismos datos

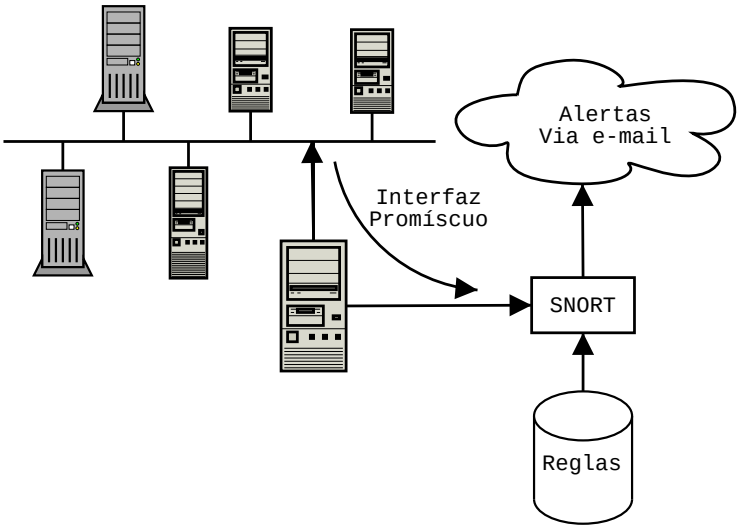

Figura 4: Esquema de funcionamiento de SNORT

Es importante la puntualización de guardar las sumas en un soporte físico fuera de la máquina ya que si las dejamos en la misma y alguien realiza una intrusión, podría modificarlas para que encajasen con su programa con código malicioso.

Este sistemas de detección de intrusos no es en tiempo real (se pasa cuando se tiene una sospecha de que algo va mal o cada cierto tiempo) y puede encajar en los sistemas basados en el objetivo (detectando anomalías).

5.3. SNORT

SNORT es un sistema de detección de intrusos en tiempo real y basado en red muy potente. Este sistema sigue el planteamiento de colocar una máquina con un interfaz promíscuo que monitorice el tráfico que circula por la red, de este modo SNORT busca patrones que hagan presagiar que se esta desencadenando un ataque sobre la red que este monitoriza.

Al igual que logcheck y siguiendo la arquitectura general, el sistema incorpora paquetes de reglas para realizar chequeos determinados sobre el tráfico de red, en este caso categorizados en diversos (y numerosos) grupos como `smtp.rules`, `ddos.rules`, etcétera.

Otra de las grandes virtudes de SNORT es que incorpora un sistema bastante sencillo para escribir nuestras reglas, de modo que podemos adaptarlo a nuestros requerimientos reescribiendo las reglas para

los incidentes que deseamos monitorizar.

Un ejemplo de regla de SNORT:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-ATTACKS ps command
attempt"; flags:A+; uricontent:"/bin/ps"; nocase; sid:1328; rev:1;
classtype:web-application-attack;)
```

Con este lenguaje se nos permite introducir no solo el protocolo o el puerto al que va destinado el paquete, también podemos indicar el contenido de este, flags determinados de los protocolos, etcétera, de modo que hace el programa extremadamente flexible.

6. Conclusiones

En esta ponencia hemos visto tanto el esquema general de la detección de intrusos como ejemplos detallados sobre software libre y Linux que nos han ilustrado por una parte la potencia que puede alcanzar un producto de software libre (con todas sus ventajas) y por otra cada una de las categorías expuestas de modo general en la introducción.

Sin embargo y aunque los sistemas de detección de intrusos son un buen medio para mantenernos alerta de lo que ocurre en nuestra red en cuanto a ataques, este medio es del todo inutil si no tomamos las precauciones suficientes en aspectos mucho más básicos como tener buenas passwords en nuestros sistemas, un sistema de firewalling correcto, parchear aplicaciones o tener un backup siempre disponible.