Sistemas de Detección de Intrusos

Los sistemas de detección de intrusiones, bien sea dispuestos como software que se ejecuta en servidores y estaciones de trabajo, bien instalados en la infraestructura de red, monitorizan la actividad de los sistemas en busca de violaciones de la política de seguridad, tales como ataques de denegación de servicio, sustracción o modificación de información delicada, etc. Este artículo hace una introducción los IDS y los clasifica por tipos.

Introducción

Las organizaciones dependen cada vez más de sistemas informáticos para su funcionamiento diario. La existencia de atacantes, tanto internos como externos, que pretenden acceder ilegítimamente a sistemas informáticos, sea para sustraer información confidencial, o para modificar o eliminar información, sea con un interés concreto o por simple entretenimiento, hace que la seguridad sea algo que ha de evolucionar a la par que la tecnología se desarrolla.
Los cortafuegos son una herramienta indispensable para hacer ejecutar las políticas de empresa, pero el hecho de que suelen realizar un análisis muy superficial de la información que circula por la red (generalmente, se quedan a nivel de red), hace que muchos ataques sean simplemente invisibles para ellos.
En los 80 comenzaron los primeros desarrollos de programas que monitorizaban el uso de sistemas y redes. En los últimos años se ha producido un avance muy grande en esta área, y la mayoría de las empresas dedicadas a la seguridad ofrecen productos para la detección de intrusiones.
Los sistemas de detección de intrusiones (IDS) están constantemente vigilando, e incorporan mecanismos de análisis de tráfico y de análisis de sucesos en sistemas operativos y aplicaciones que les permiten detectar intrusiones en tiempo real.
Un IDS puede ser un dispositivo *hardware* autocontenido con una o varias interfaces, que se conecta a una o varias redes; o bien una aplicación que se ejecuta en una o varias máquinas y analiza el tráfico de red que sus interfaces ven y/o los eventos generados por el sistema operativo y las aplicaciones locales.
Para hablar sobre detección de intrusiones hay que definir qué entendemos por intrusión. Las intrusiones se definen en relación a una política de seguridad: una intrusión es una violación de la política de seguridad establecida. A menos que se conozca qué está permitido en un sistema y qué no, no tiene sentido hablar de detección intrusiones.
De manera más concisa se puede definir una intrusión como un conjunto de acciones deliberadas dirigidas a comprometer la integridad (manipular información), confidencialidad (acceder ilegítimamente a información) o disponibilidad de un recurso (perjudicar o imposibilitar el funcionamiento de un sistema).

Clasificación de los IDS

Los IDS se pueden clasificar desde varios puntos de vista. A continuación describimos las diversas clasificaciones posibles.

El paradigma de detección de anomalías puede detectar incluso ataques desconocidos.

Tipos de detección

En primer lugar los clasificaremos según la manera en que detectan las intrusiones.
Categorizamos las intrusiones en dos tipos principales, cuya distinción es importante porque nos conducirán a sistemas de detección esencialmente muy diferentes.
• Los **usos indebidos** son ataques bien definidos contra debilidades conocidas de los sistemas. Se los puede detectar buscando la ocurrencia de determinadas acciones concretas.
• Las **anomalías** se basan en la observación de desviaciones de los patrones de uso normales en el sistema. Se las detecta construyendo previamente un perfil del sistema a monitorizar y posteriormente estudiando las desviaciones que se produzcan con respecto a este perfil.
Las intrusiones por uso indebido siguen patrones bien definidos, por lo que se pueden detectar realizando búsqueda de patrones en el tráfico de red y en los ficheros de registro.
Las intrusiones por anomalía se detectan observando desviaciones significativas del comportamiento habitual. Para ello se mide una serie de parámetros (carga de CPU, número de conexiones de red en una unidad de tiempo, número de procesos, entre otros). Considerando que una intrusión involucrará un uso anormal del sistema, se pueden detectar las violaciones de seguridad a partir de patrones anormales de uso.
Los detectores de anomalías conocen, bien porque han sido programados por un experto, bien porque han pasado por una fase previa de **aprendizaje**, la actividad que resulta “normal” en el seno de un sistema. Mediante métodos estadísticos se intentará posteriormente comparar la información recibida en cada instante con el modelo de actividad válida, y aquello que se aparte excesivamente será etiquetado como intrusión. Esta comparación se puede realizar por técnicas estadísticas, por sistemas expertos basados en reglas, con redes neuronales, o con algún otro tipo de reconocimiento de patrones que pueda emitir con una certeza razonable si una determinada secuencia de eventos en un sistema forma parte del funcionamiento ordinario del mismo.

Sistemas de Detección de Intrusos

Es difícil detectar intrusiones por anomalías. No hay patrones fijos que se puedan monitorizar, por lo que se usan aproximaciones "borrosas" que suelen producir altas tasas de error. La correlación de los datos recibidos por los sensores es en la actualidad un área de investigación sujeta a estudio. Se persigue minimizar el número de falsos positivos (falsas alarmas) y de falsos negativos (ataques reales que pasan inadvertidos al sistema).
El paradigma de detección de anomalías parece bastante potente, pues en principio es capaz de detectar todo tipo de ataques, incluso ataques desconocidos hasta la fecha de su ocurrencia. En el caso de sistemas basados en reglas, exigen de un experto que pueda introducir correctamente dicho conjunto, que ha de ser periódicamente actualizado conforme las prácticas varíen. En el caso de sistemas basados en aprendizaje puede ocurrir que un atacante varíe muy lentamente su comportamiento para hacer casar una actividad maliciosa dentro de lo aceptable por el nuevo modelo aprendido. Los sistemas informáticos son por naturaleza muy cambiantes y los detectores de anomalías pueden producir una tasa de falsos positivos inaceptable.

La detección de "signaturas" conocidas llega a alcanzar tasas despreciables de falsos positivos.

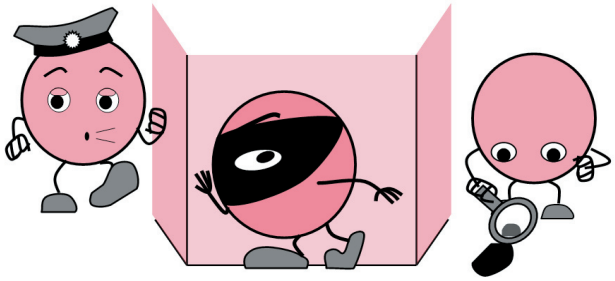
En la práctica se han extendido más los detectores de usos indebidos, que se basan en una base de datos de ataques conocidos, con una serie de reglas o "signaturas" que caracterizan los ataques y que permiten aseverar con prácticamente total certeza que se está intentando perpetrar un ataque. Estos sistemas solo pueden detectar fallos conocidos, para los que se haya introducido la signatura correspondiente en la lista. Dado que cada día aparecen nuevas vulnerabilidades, es importante que estos sistemas dispongan de mecanismos para actualizar frecuentemente la base de signaturas.

Fuentes de información

Dependiendo de las fuentes de información que se utilicen, los sensores usados por los IDS se clasifican en dos tipos: de red y de máquina. Cada tipo tiene unas capacidades diferentes en cuanto a los eventos detectables, por lo que en la práctica los IDS suelen nutrirse de sensores de ambos tipos. En la terminología tradicional de IDS, se habla de NIDS (Sistemas de Detección de Intrusos de Red) y de HIDS (Sistemas de detección de intrusos de máquina). En los sistemas híbridos o distribuidos, que abarcan más de un solo nodo, se habla de **sensores**: un solo sistema de detección de intrusiones puede alimentarse de más de un sensor. Como la mayoría de los sistemas de IDS comerciales son aparatos independientes dotados de sensores de red que se conectan sin tener que instalar nada en ninguna otra máquina, se ha abusado bastante del término NIDS.

1. NIDS

Sistemas de detección de intrusos por red. Estos sistemas disponen de una o varias interfaces de red conectadas a determinados puntos estratégicos de la red. Monitorizan el tráfico que pasa por dichos puntos en busca de tráfico malicioso. Aunque estos sistemas en principio son dispositivos absolutamente pasivos, con frecuencia se colocan los NIDS en cortafuegos y enrutadores, de manera que el propio sistema puede forzar el cierre de conexiones y modificar reglas de filtrado de una manera más directa. Mediante uno solo de estos sistemas se puede monitorizar el tráfico tanto interno como externo de una red para muchas máquinas.
Los NIDS no suelen controlar toda la red sino determinados puntos estratégicos. La mayoría de las redes hoy en día son conmutadas, así que colocar los sensores de red suele implicar utilizar conmutadores especiales con un puerto "monitor" que reproduce todo el tráfico recibido en cualquiera de los puertos.



Los IDS, correctamente utilizados, ayudan a mejorar la seguridad de nuestras redes, pero no debemos descuidar los cortafuegos ni dejar de actualizar el software de las máquinas.

Este tipo de sistemas son bastante rápidos de instalar y mantener, y no dependen del sistema operativo instalado en las máquinas cubiertas. Suelen ser invisibles para los atacantes, por lo que los registros de sucesos que almacenan son poco vulnerables a la eliminación o alteración maliciosa, y suponen un recurso valioso para el almacenamiento de pruebas.
Diferentes ubicaciones de los NIDS nos proporcionarán diferentes perspectivas de la seguridad de la red. Colocados fuera del cortafuegos permiten evaluar los ataques que se intentan producir aunque no alcancen a los servidores internos, mientras que si se colocan en el interior del cortafuegos nos permiten evaluar si este está bien configurado.

2. HIDS

Sistemas de detección de intrusos de máquina. Así como los NIDS se instalan en determinados puntos de la infra-

Sistemas de Detección de Intrusos

estructura de red, los HIDS se instalan en las máquinas que componen la red: tanto servidores como estaciones de trabajo. Un sensor, instalado directamente como un módulo sobre una máquina, dispone de información de mayor nivel semántico que los NIDS: llamadas al sistema, eventos complejos dentro de aplicaciones de alto nivel, etc. Un sistema basado únicamente en red tendría que ser mucho más complejo para "entender" la gran diversidad de protocolos que existen, y los que se implementan por encima de éstos. Por otra parte, la tendencia actual al uso de conexiones encriptadas, de indiscutible interés para mejorar la seguridad de los sistemas, hace que un sistema que solo escuche la red disponga de muy poca información para distinguir el tráfico malicioso del aceptable. El tráfico en una conexión SSH o SSL es absolutamente inaccesible a un NIDS, aunque en el caso de SSL se han desarrollado cortafuegos que interceptan las conexiones, realizando una especie de ataque "hombre en el medio" que le permite analizar el contenido de conexiones que de otra manera sería inaccesible.

Los HIDS tienen acceso a los archivos de registro de lo que realmente sucedió, por lo que pueden conocer de manera fiable si un ataque fue exitoso o no, información generalmente no disponible para los NIDS.

Un sensor de máquina dispone de información específica del sistema y las aplicaciones, como inicios/cierres de sesión, acceso a ficheros, llamadas al sistema (pueden utilizarlas para saber el disco libre, la ocupación de la red, etc), y otros eventos, incluyendo aquellos que se originan localmente sin generar tráfico de red.

Tienen sobre los NIDS la ventaja de que permiten acceder a la información que por la red transita encriptada y que por lo tanto es opaca a ellos (p. ej., peticiones HTTPS inválidas).

Modo de análisis	Detectores de usos indebidos	
	Detectores de anomalías	
Tipo de sensores	De red	
	De máquina	Sistema operativo
		De aplicación
		Hardware
Tiempo de ejecución	Periódicos	
	De tiempo real	
Tipo de respuesta	Activos	
	Pasivos	
Arquitectura	Centralizados	
	Distribuidos	

Tabla 1: Posibles clasificaciones de los Sistemas de Detección de Intrusos.

Periódicos o de tiempo real

Así como los NIDS suelen dar respuesta en tiempo real, los primeros HIDS se ejecutaban periódicamente para buscar indicios de intrusión. Después se fue reduciendo el intervalo entre la ocurrencia del evento y su análisis, hasta el punto que es posible gestionar los eventos en el instante de su registro. Los sistemas de red implementados como parte de la pila de red de las máquinas protegidas ofrecen las mismas prestaciones de respuesta inmediata (con posibilidad de cancelación de conexiones) que los NIDS.

Activos o pasivos

Los primeros IDS eran pasivos, se limitaban a informar de los intentos de intrusión al administrador. De poco sirve detectar un ataque para que horas después el administrador reciba un mensaje que informe de que se vio la intrusión pero no se intentó hacer nada por abortarla. Los IDS activos son capaces de tomar acciones correctivas orientadas a detener ataques en el mismo instante en que se producen.

Centralizados o distribuidos

Cuando la red de una organización adquiere una envergadura determinada, ya no es factible analizar todo el tráfico en un solo punto sin producir una degradación del rendimiento. En tal caso se instalan sistemas distribuidos, que disponen de varios sensores repartidos por diversas máquinas y puntos de la red, que se comunican con un nodo central donde se reciben todas las informaciones relevantes y donde se cruzan los datos para disponer de una visión más amplia del sistema como conjunto y detectar con mayor fiabilidad eventuales ataques. Esto permite producir además una única respuesta a intrusiones visibles desde varios puntos de la red.

Evasión de IDS

Es posible que el sistema no sea capaz de detectar una determinada instancia de ataque conocido al ser incapaz de encontrar la coincidencia con el patrón de búsqueda, si el atacante se las arregla para introducir pequeñas variaciones en su interacción con la máquina precisamente con el objetivo de evadir el IDS. Por ejemplo, algunas estrategias de evasión explotan leves diferencias en la manera en que la pila TCP reensambla fragmentos, o la manera en que se procesan paquetes inválidos, etcétera. La mayoría de los productos IDS de hoy en día incluyen protecciones contra las técnicas de evasión de IDS.

Sistemas de decepción

Son un tipo especial de sistema de detección de intrusiones orientados a atraer la atención de potenciales intrusos para que no ataquen a los sistemas reales y para obtener información acerca de sus métodos. Son los llamados *honeypots* (tarros de miel): máquinas simuladas, verosímiles y relativamente poco ocultas. Dado que ningún usuario legítimo debería querer jamás intentar conectarse

Sistemas de Detección de Intrusos

a un *honeypot*, toda conexión al mismo puede informarse inmediatamente y etiquetarse como un intento de intrusión. Los *honeypots* están configurados para registrar los eventos extensamente. La irrupción de un intruso en estas máquinas permite a los administradores obtener información sobre su *modus operandi*, e incluso recabar pruebas o indicios que pudieran inculpar al delincuente en un juicio.

Análisis forense

Los IDS ofrecen un interesante servicio para el análisis forense después de la consumación de ataques. Es posible que un IDS no haya sido capaz de detener la acción de un atacante, pero sí puede haber guardado un registro de los mensajes que transitaron por la red a tal efecto. Aunque cualquier atacante que tenga cierto nivel hará todo lo posible por borrar sus huellas, falsificar direcciones, explotar máquinas de terceros para enmascararse, etcétera, toda información que se almacene puede ayudar a seguir la pista del atacante, a mejorar los sistemas de detección y reacción automatizada a dichos ataques, e incluso como indicios ante instancias judiciales.

Algunas herramientas disponibles

Snort

Snort, uno de los sistemas más utilizados actualmente, es un sistema de código abierto de detección de intrusiones de red, capaz de llevar a cabo análisis de tráfico en tiempo real y registro de paquetes en redes IP. Puede efectuar análisis de protocolos, búsqueda de cadenas o patrones en el contenido y puede utilizarse para detectar una gran variedad de ataques y sondeos, tal como desbordamientos de búfer, escaneos invisibles, ataques CGI, sondeos SMB, intentos de determinación del sistema operativo, y otros.
Snort utiliza un flexible lenguaje de reglas para describir el tráfico que debería recoger o pasar, así como un motor de detección que hace uso de una arquitectura de plugins modular. Entre su base de reglas incluye miles de comprobaciones en busca de ataques de denegaciones de servicio. Ofrece la posibilidad de alertar en tiempo real, al incorporar mecanismos para registrar a syslog, a fichero, a sockets Unix, o mediante Samba, enviar mensajes emergentes a clientes Windows.
Además de ser un sistema completo de detección de intrusiones de red, sirve como analizador de paquetes al estilo de *tcpdump*, y como herramienta para registrar el tráfico. Se puede compilar en una veintena de plataformas distintas, tanto sistemas Unix como Win32.

Prelude

Snort es el IDS de red libre más potente, pero en su arquitectura no contempla la posibilidad de usar sensores de máquina, lo cual motivó la aparición del proyecto, también libre, Prelude, que utiliza una arquitectura distribuida, con canales autenticados y encriptados, y sensores para diversos sistemas operativos. Prelude no pretende reinventar la rueda en IDSs de red, y de hecho es capaz de nutrirse de Snort, e incluso incluye él mismo un motor que utiliza los ficheros de reglas de su predecesor.

Intrudec

El ITI está desarrollando un prototipo de sistema de detección de intrusiones, Intrudec. Se trata de una arquitectura distribuida, con tolerancia a fallos, altamente modular, con soporte para sensores tanto de red como de máquina, que se comunican de manera segura para permitir la correlación de los diversos eventos ocurridos en distintos puntos de la red y en los distintos sistemas monitorizados. Para la correlación se utilizan diversos algoritmos, cuyo desarrollo y ajuste constituyen la labor de investigación principal del grupo de Sistemas Fiables en el área de la detección de intrusiones. Intrudec complementa al proyecto Tigerweb, que este grupo ha estado desarrollando y manteniendo en los últimos dos años. Tigerweb es un sistema de detección remota de vulnerabilidades accesible vía web que proporciona informes bien organizados y en castellano, orientados a ser entendidos por personal no experto en el área de la seguridad de los sistemas informáticos (Actualidad TIC, vol 2, págs. 4-7).

Futuro y conclusiones

Los IDS son una herramienta más que podemos utilizar para mejorar la seguridad de nuestros sistemas. Los IDS no reemplazan a los cortafuegos, ni nos evitan la tarea de mantener las máquinas actualizadas y correctamente configuradas.
Los propios IDS, en especial si se basan en búsqueda de patrones, han de mantenerse puntualmente actualizados. Las alertas generadas han de ser cuidadosamente analizadas para tomar las medidas pertinentes lo antes posible -de ahí la importancia de que los sistemas tengan una tasa baja de falsos positivos.
Existen actualmente fuertes críticas a los IDS estándar, por el hecho de que en principio un IDS detecta intrusiones pero no toma medidas correctivas. Esto ha llevado a algunos expertos a afirmar que los IDS no resultan eficaces, sobre todo considerando los costes de implantación y mantenimiento, y que su futuro puede ser virar hacia los IPS (Sistemas de Prevención de Intrusiones), productos combinados con cortafuegos que sí son capaces de adoptar medidas correctivas inmediatas (cortar conexiones, cambiar reglas de filtrado...).

Autor: Raúl Salinas
Más información: seguridad@iti.upv.es