Sistemas de detección de intrusos

Qué es un sistema de detección de intrusos

Un sistema de detección de intrusos (IDS por sus siglas en inglés - Intrusion Detection System) es un programa o dispositivo activo que monitoriza la actividad de un sistema o una red en busca de intentos de intrusión. Es un mecanismo que, sigilosamente, escucha el tráfico de la red para detectar actividades anormales o sospechosas.

Definiremos intrusión como cualquier acción que intente comprometer la integridad, confidencialidad o disponibilidad de un recurso. De aquí podemos extraer que que una intrusión no tiene por qué ser únicamente un acceso no autorizado a una máquina, sino que también puede ser una denegación de servicio.

Existen dos familias importantes: **N-IDS** (sistemas de detección de intrusiones de red), que garantiza la seguridad dentro de la red, y **H-IDS** (sistema de detección de intrusiones en el *host*), que garantiza la seguridad en el *host*.

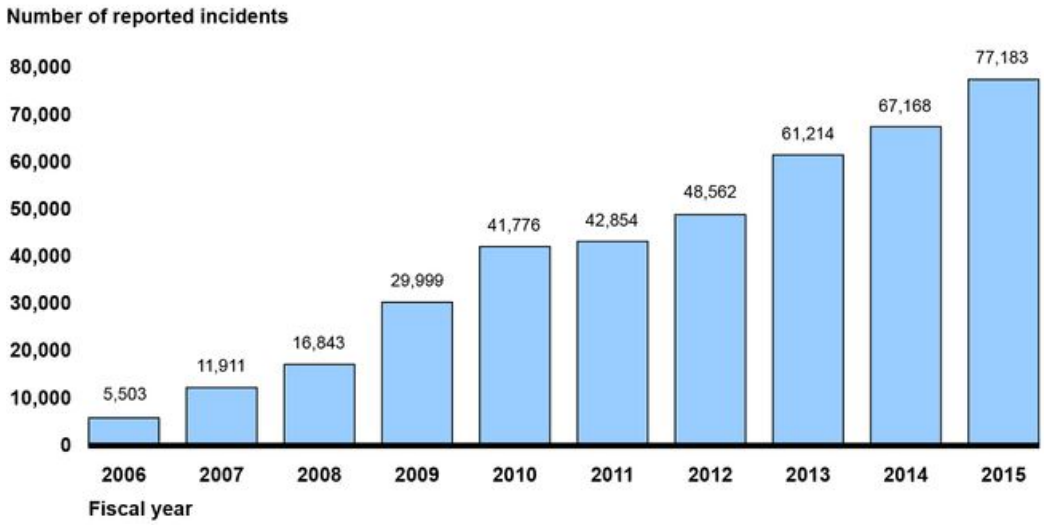
Características de un IDS

Cualquier sistema de detección de intrusos debería contar con las siguientes características:

1. Funcionar continuamente sin supervisión humana.
2. Ser tolerante a fallos; es decir, ser capaz de sobrevivir a una caída del sistema.
3. Ser resistentes a perturbaciones.
4. Debe imponer mínima sobrecarga sobre el sistema.
5. Debe observar desviaciones sobre el comportamiento estándar.
6. Debe ser fácilmente adaptable al sistema ya instalado.
7. Debe hacer frente a los cambios del comportamiento del sistema según se añaden nuevas aplicaciones.
8. Debe ser difícil de engañar.

Motivación para el uso de un IDS

No es sorprendente que el número de incidentes de ciberseguridad aumenten año tras año. Lo preocupante, no obstante, es que no solo aumente el número sino la gravedad de los mismos. El año pasado “presenciamos” algunos de los peores ataques que se recuerdan, en mayo y junio hubo dos ataques de ransomware que afectaron directamente a organizaciones gubernamentales como la NHS Británica o al gobierno Ucraniano. En el mes de agosto un ataque de denegación de servicio distribuido dirigido contra DreamHost (proveedor de alojamiento web y nombres de dominio) logró tirar gran parte de sus servidores impidiendo a muchos usuarios el acceso a plataformas como Twitter o la página web de Whatsapp.



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

2017 Incident Highlights

159,700 total cyber incidents in 2017 (OTA)

93% of breaches could have been prevented (OTA)

18.2% increase in reported breach incidents (RBS)

7 billion records exposed in first 3 quarters (RBS)

$5 billion financial impact of ransomware (CV)

90% rise in business targeted ransomware (Symantec)

$5.3 billion in global BEC losses (FBI)

Worldwide estimates. Sources: (OTA) Online Trust Alliance, (RBS) Risk Based Security, Cybersecurity Ventures (CV)

Resulta evidente la necesidad de implantación de sistemas de prevención. Más aún tras el conocimiento de datos como el de que el 93% de los incidentes podrían haberse evitado. Los motivos no son pocos. Si un atacante es consciente de la existencia de sistemas que delaten su presencia y la castiguen, en algunos casos se replanteará sus intenciones.

Un IDS puede detectar cuando un atacante ha intentado penetrar en un sistema explotando un fallo no corregido. De esta forma, podríamos avisar al administrador para que llevara a cabo un backup del sistema inmediatamente, evitando así que se pierda información valiosa.

Cuando un individuo ataca un sistema, lo hace típicamente en fases predecibles. En la primera fase, el atacante hace pruebas y examina el sistema o red en busca de un punto de entrada óptimo. En sistemas o redes que no disponen de un IDS, el atacante es libre de examinar el sistema con un riesgo mínimo de ser detectado. Esto le facilita la búsqueda de un punto débil en nuestra red. Un IDS observará estas pruebas, las identificará como sospechosas, podrá activamente bloquear el acceso del atacante al sistema objetivo y avisará al personal de seguridad de lo ocurrido para que tome las acciones pertinentes.

Incluso cuando los IDSs no son capaces de bloquear ataques, pueden recoger información relevante sobre éstos. Esta información puede, bajo ciertas circunstancias, ser utilizada como prueba en actuaciones legales. También se puede usar esta información para corregir

fallos en la configuración de seguridad de los equipos o en la política de seguridad de la organización.

Clasificación de IDSes

Se pueden clasificar en dos grandes grupos: en función de qué sistemas vigilan o en función de cómo lo hacen.

1. Qué sistemas vigilan: hay dos grupos: los que analizan actividades de una única máquina y los que lo hacen de una subred. De estos últimos hay que saber que un IDS no tiene por qué ubicarse en todas las máquinas.

    a. IDSes basados en red: monitorizan los paquetes que circulan por una red en busca de elementos que denoten un ataque contra alguno de los sistemas que la conforman. Los IDSes basados en red pueden alojarse en un host de la red en un elemento de la que dependa la misma, como un router. Esta característica, sin embargo, no acota la monitorización a la máquina que lo aloja.
    b. IDSes basados en host: realizan su función protegiendo un único sistema. Es un proceso que trabaja en segundo plano buscando patrones que puedan denotar un intento de intrusión y alertando o actuando. Este grupo se puede dividir a su vez en tres subgrupos: verificadores de integridad del sistema (SIV), que está encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas; monitores de registros (LFM), que monitorizan los archivos de log generados por los programas de una máquina en busca de patrones que indiquen una intrusión; sistemas de decepción, que se encargan de simular servicios con problemas de seguridad de forma que, si alguien intenta hacer una intrusión, se guarden todas sus actividades.
2. Cómo vigilan:
    a. Detección de anomalías: el sistema supone que una intrusión se puede ver como una anomalía del sistema, por lo que si fuéramos capaces de establecer un perfil del comportamiento habitual del sistema, seríamos capaces de detectar las intrusiones.
    b. Detección de usos indebidos: el sistema presupone que podemos establecer patrones para los diferentes ataques conocidos y alguna variación.

Técnicas para detectar intrusiones

1. Verificación de la lista de protocolos: algunas formas de intrusión utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos.

2. Verificación de los protocolos de la capa de aplicación: algunas formas de intrusión emplean comportamientos de protocolos no válidos.
3. Reconocimiento de ataques de comparación de patrones: consiste en la identificación de una intrusión al examinar un paquete y reconocer la secuencia que corresponde a una firma específica.

Demo

Instalación de Snort en Ubuntu 16.04:
https://www.upcloud.com/support/installing-snort-on-ubuntu/

En el fichero local.rules, añadimos la siguiente regla para detectar un ataque de denegación de servicio:

```
alert tcp any any -> $HOME_NET 80 (flag: S; msg:”Posible ataque DoS”; flow: stateless; threshold: type both, track by_dst, count 70, second 10; sid:10001; rev:1;)
```

Y la siguiente regla para detectar posibles ataques de fuerza bruta a SSH:

```
alert tcp any any -> $HOME_NET 22 (msg:"Posible ataque por fuerza bruta a SSH"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid:10000001; rev: 1;)
```

Las opciones “count” y “second” pueden variar en función del tráfico que esperemos recibir.

Enlaces

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

https://www.rediris.es/cert/doc/pdf/ids-uv.pdf

https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

https://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos

https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

https://www.techrepublic.com/article/major-ddos-attack-lasts-297-hours-as-botnets-bombard-businesses/

https://www.upcloud.com/support/installing-snort-on-ubuntu/