IDS/IPS - Introducción

Como todas las vulnerabilidades no son conocidas, así como tampoco son conocidos los posibles ataques, se han desarrollado productos para detectar tanto las posibles vulnerabilidades de los programas instalados en los ordenadores, del sistema operativo como de servicios de red, como los posibles ataques que se pueden perpetrar.

Han surgido detectores de ataques, que actúan como centinelas.

Firewalls vs IDS

Es entonces cuando hablamos de los Intrusion Detection Systems (IDS) e Intrusion Prevention Systems (IPS). De ahora en adelante, ambos serán referenciados como "IDS".

Un IDS es un sistema que intenta detectar y alertar sobre las intrusiones intentadas en un sistema o en una red, considerando intrusión a toda actividad no autorizada o que no debería ocurrir en ese sistema. Según esta definición, muchos podrían pensar que ese trabajo ya se realiza mediante los firewalls. Pero ahora veremos las diferencias entre los dos componentes y como un IDS es un buen complemento de los cortafuegos.

La principal diferencia, es que un cortafuegos es una herramienta basada en la aplicación de un sistema de restricciones y excepciones sujeta a muchos tipos de ataques, desde los ataques "tunneling"(saltos de barrera) a los ataques basados en las aplicaciones. Los cortafuegos filtran los paquetes y permiten su paso o los bloquean por medio de una tabla de decisiones basadas en el protocolo de red utilizado.

Las reglas verifican contra una base de datos que determina si está permitido un protocolo determinado y permite o no el paso del paquete basándose en atributos tales como las direcciones de origen y de destino, el número de puerto, etc... Esto se convierte en un problema cuando un atacante enmascara el tráfico que debería ser analizado por el cortafuegos o utilizar un programa para comunicarse directamente con una aplicación remota. Estos aspectos se escapan a las funcionalidades previstas en el diseño inicial de los cortafuegos. Es aquí donde entran los IDS, ya que estos son capaces de detectar cuando ocurren estos fallos.

Definiciones

Como se ha descrito en el apartado anterior, un IDS es un software que monitorea el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información.

Algunas de las características deseables para un IDS son:

- Deben estar continuamente en ejecución con un mínimo de supervisión.
- Se deben recuperar de las posibles caídas o problemas con la red.
- Debe poderse analizar él mismo y detectar si ha sido modificado por un atacante.
- Debe utilizar los mínimos recursos posibles.
- Debe estar configurado acorde con la política de seguridad seguida por la organización.
- Debe de adaptarse a los cambios de sistemas y usuarios y ser fácilmente actualizable.

Tipos de IDS

Existen varios tipos de IDS, clasificados según el tipo de situación física, del tipo de detección que posee o de su naturaleza y reacción cuando detecta un posible ataque.

Por situación

Según la función del software IDS, estos pueden ser:

- NIDS (Network Intrusion Detection System)
- HIDS (Host Intrusion Detection System)

Los NIDS analizan el tráfico de la red completa, examinando los paquetes individualmente, comprendiendo todas las diferentes opciones que pueden coexistir dentro de un paquete de red y detectando paquetes armados maliciosamente y diseñados para no ser detectados por los cortafuegos. Pueden buscar cual es el programa en particular del servidor web al que se está accediendo y con qué opciones y producir alertas cuando un atacante intenta explotar algún fallo en este programa. Los NIDS tienen dos componentes:

- Un sensor: situado en un segmento de la red, la monitoriza en busca de tráfico sospechoso
- Una consola: recibe las alarmas del sensor o sensores y dependiendo de la configuración reacciona a las alarmas recibidas.

Las principales ventajas del NIDS son:

- Detectan accesos no deseados a la red.
- No necesitan instalar software adicional en los servidores en producción.
- Fácil instalación y actualización por que se ejecutan en un sistema dedicado.

Como principales desventajas se encuentran:

- Examinan el tráfico de la red en el segmento en el cual se conecta, pero no puede detectar un ataque en diferentes segmentos de la red. La solución más sencilla es colocar diversos sensores.
- Pueden generar tráfico en la red.
- Ataques con sesiones encriptadas son difíciles de detectar.

En cambio, los HIDS analizan el tráfico sobre un servidor o una PC, se preocupan de lo que está sucediendo en cada host y son capaces de detectar situaciones como los intentos fallidos de acceso o modificaciones en archivos considerados críticos. Las ventajas que aporta el HIDS son:

- Herramienta potente, registra comandos utilizados, ficheros abiertos,...
- Tiende a tener menor número de falsos-positivos que los NIDS, entendiendo falsos-positivos a los paquetes etiquetados como posibles ataques cuando no lo son.
- Menor riesgo en las respuestas activas que los IDS de red.
- Los inconvenientes son:
- Requiere instalación en la máquina local que se quiere proteger, lo que supone una carga adicional para el sistema.
- Tienden a confiar en las capacidades de auditoría y logging de la máquina en sí.

Según los modelos de detección

Los dos tipos de detecciones que pueden realizar los IDS son:

- Detección del mal uso.
- Detección del uso anómalo.

La detección del mal uso involucra la verificación sobre tipos ilegales de tráfico de red, por ejemplo, combinaciones dentro de un paquete que no se podrían dar legítimamente. Este tipo de detección puede incluir los intentos de un usuario por ejecutar programas sin permiso (por ejemplo, "sniffers"). Los modelos de detección basado en el mal uso se implementan observando cómo se pueden explotar los puntos débiles de los sistemas, describiendolos mediante unos patrones o una secuencia de eventos o datos ("firma") que serán interpretados por el IDS.

La detección de actividades anómalas se apoya en estadísticas tras comprender cuál es el tráfico "normal" en la red del que no lo es. Un claro ejemplo de actividad anómala sería la detección de tráfico fuera de horario de oficina o el acceso repetitivo desde una máquina remota (rastreo de puertos). Este modelo de detección se realiza detectando cambios en los patrones de utilización o comportamiento del sistema. Esto se consigue realizando un modelo

estadístico que contenga una métrica definida y compararlo con los datos reales analizados en busca de desviaciones estadísticas significantes.

Según su naturaleza

Un tercer y último tipo básico de clasificación sería respecto a la reacción del IDS frente a un posible ataque:

- ❏ Pasivos.
- ❏ Reactivos.

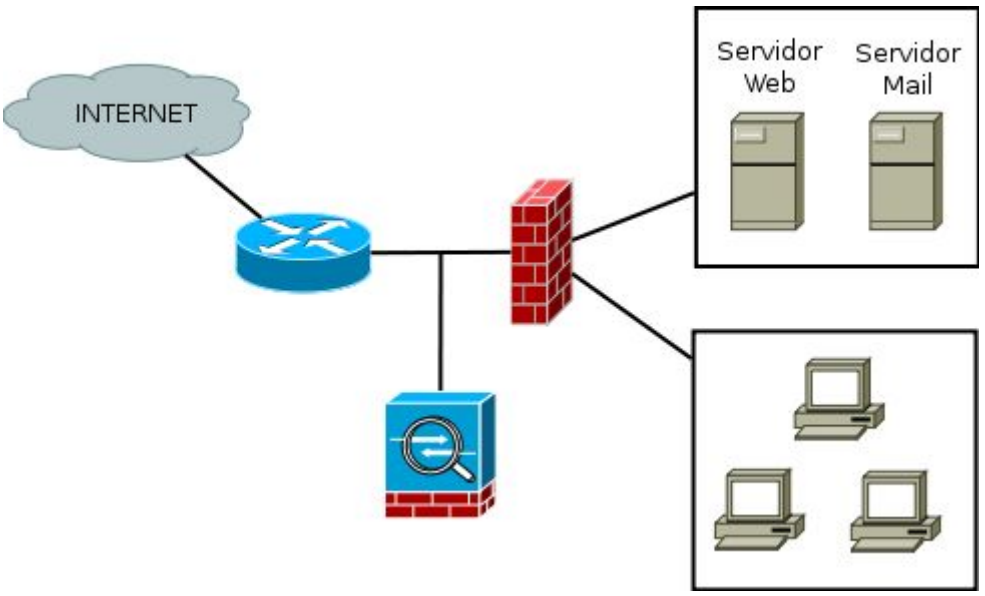
Los IDS pasivos detectan una posible violación de la seguridad, registran la información y genera una alerta.

Los IDS reactivos están diseñados para responder ante una actividad ilegal, por ejemplo, sacando al usuario del sistema o mediante la reprogramación del cortafuegos para impedir el tráfico desde una fuente hostil. A este tipo de sistemas se los suele llamar Intrusion Prevention System (IPS), o Sistema de Prevención de Intrusiones.

Topologías de IDS

Existen muchas formas de añadir las herramientas IDS a nuestra red, cada una de ellas tiene su ventaja y su desventaja. La mejor opción debería ser un compendio entre coste económico y propiedades deseadas, manteniendo un alto nivel de ventajas y un número controlado de desventajas, todo ello de acuerdo con las necesidades de la organización.

Por este motivo, las posiciones de los IDS dentro de una red son varias y aportan diferentes características. A continuación vamos a ver diferentes posibilidades en una misma red. Imaginemos que tenemos una red donde un cortafuegos nos divide la Internet de la zona desmilitarizada (DMZ – Demilitarized Zone), y otro que divide la DMZ de la intranet de la organización como se muestra en el dibujo 1. Por zona desmilitarizada entendemos la zona que debemos mostrar al exterior, la zona desde la cual mostramos nuestros servicios o productos:



Red con IDS simple

Si situamos un IDS antes del cortafuegos exterior permitiría detectar el rastreo de puertos de reconocimiento que señala el comienzo de una actividad maliciosa, y obtendríamos como ventaja un aviso prematuro. Sin embargo, si los rastreos no son seguidos por un ataque real, se generará un numeroso número de alertas innecesarias con el peligro de comenzar a ignorarlas.

Si optamos por colocar el IDS en la zona desmilitarizada (DMZ) tendríamos como ventaja la posibilidad de adecuar la base de datos de atacantes del NIDS para considerar aquellos ataques dirigidos a los sistemas que están en la DMZ (servidor web y servidor de correo) y configurar el cortafuegos para bloquear ese tráfico.

Así mismo, un NIDS dentro de la red, por ejemplo, de Recursos Humanos podría monitorear todo el tráfico para fuera y dentro de esa red. Este NIDS no debería ser tan poderoso como los comentados anteriormente, puesto que el volumen y el tipo de tráfico es más reducido.

Autor: Fabian Martinez Portantier

Fuentes:

- https://seguridadyredes.wordpress.com