IDS/IPS
INFORME

16/12/2009
ESCUELA POLITÉCNICA NACIONAL
Diego Jefferson Chacón Herrera

INFORME

TEMA: IDS/IPS

OBJETIVOS:

- Consultar, analizar y discutir las ventajas que se pueden obtener con la implementación de IDS/IPS y sus respectivas configuraciones que garanticen la seguridad de la red.

- Analizar las ventajas y desventajas de la utilización de este tipo de configuraciones, y determinar el método más apropiado de implementación de éstas a través del análisis de distintos escenarios, ampliando nuestros conocimientos de seguridad en redes y favoreciendo nuestra capacitación laboral.

MARCO TEÓRICO:

SISTEMA DE DETECCIÓN DE INTRUSOS

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Funcionamiento

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

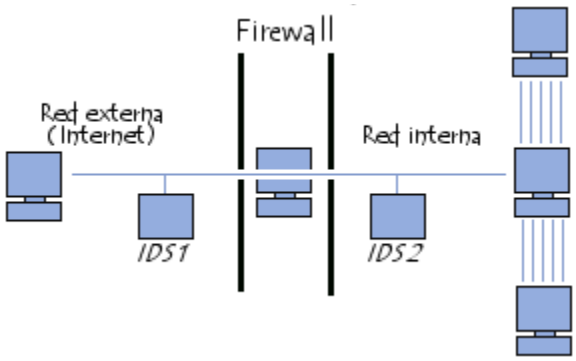

Fig. IDS configurados en una red

Tipos de IDS

Existen tres tipos de sistemas de detección de intrusos:

- HIDS (HostIDS): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.
- NIDS (NetworkIDS): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.
- DIDS (DistributedIDS): sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).

Sistemas pasivos y sistemas reactivos

En un sistema pasivo, el sensor detecta una posible intrusión, almacena la información y manda una señal de alerta que se almacena en una base de datos. En un sistema reactivo, el IDS responde a la actividad sospechosa reprogramando el cortafuegos para que bloquee tráfico que proviene de la red del atacante.

Implementación

Para poner en funcionamiento un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución hardware, software o incluso una combinación de estos dos. La

posibilidad de introducir un elemento hardware es debido al alto requerimiento de procesador en redes con mucho tráfico. A su vez los registros de firmas y las bases de datos con los posibles ataques necesitan gran cantidad de memoria, aspecto a tener en cuenta.

En redes es necesario considerar el lugar de colocación del IDS. Si la red está segmentada con hub (capa 1 del modelo OSI) no hay problema en analizar todo el tráfico de la red realizando una conexión a cualquier puerto. En cambio, si se utiliza un switch (capa 2 del modelo OSI), es necesario conectar el IDS a un puerto SPAN (Switch Port Analiser) para poder analizar todo el tráfico de esta red.

SISTEMA DE PREVENCIÓN DE INTRUSOS

Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. Tiempo después, algunos IPS fueron comercializados por la empresa One Secure, la cual fue finalmente adquirida por NetScreen Technologies, que a su vez fue adquirida por Juniper Networks en 2004. Dado que los IPS fueron extensiones literales de los sistemas IDS, continúan en relación.

También es importante destacar que los IPS pueden actuar al nivel de equipo, para combatir actividades potencialmente maliciosas.

Funcionamiento

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

CONCLUSIONES:

- En función de los requerimientos y las necesidades de las redes es importante establecer y configurar servidores tanto de IDS como IPS, ya que, como una alternativa superior de

seguridad de redes estos sistemas proveerán mayor confiabilidad y robustez al desempeño y funcionamiento de éstas.

- Por tanto, es importante a la hora de escoger y configurar los dispositivos, disponer de un adecuado conocimiento en cuanto a su desempaño, características y coste, ya que se podrán aprovechar de esta manera todas las funcionalidades que puedan ofrecer.

- Sin embargo, es necesario aclarar que la administración en estos casos debe ser crucial, y que, además del establecimiento de políticas de red en las organizaciones se podrá dar una verdadera solución de seguridad a la red y sus respectivos usuarios.

RECOMENDACIONES:

- Se recomienda utilizar configuraciones, aplicaciones y programas similares de mayor complejidad o prestaciones, con el propósito de profundizar aún más los conocimientos relativos a la seguridad en redes.

- Antes de realizar cualquier modificación en los parámetros de configuración de los dispositivos de red es importante extraer copias de seguridad de la información que es relevante para la organización.

- Como administradores, seguir fielmente el cumplimiento de las políticas de seguridad de la institución, puesto que, de hacerlo, no sólo se estará garantizando el adecuado funcionamiento de la red, sino brindando entornos de trabajo justos y equitativos a todos los usuarios según las políticas establecidas.

BIBLIOGRAFÍA:

- es.wikipedia.org/.../Sistema_de_detección_de_intrusos
- Material recibido en clase
- http://es.wikipedia.org/wiki/Sistema_de_Prevención_de_Intrusos
- http://www.virusprot.com/Art40.htm
- http://es.kioskea.net/contents/detection/ids.php3
- http://www.guiaacademica.com/EDUCACION/personas/pages/mostrar_curso.aspx?action=2&idCur=22203
- http://es.kioskea.net/contents/detection/ips.php3