Anexo B

IDS - SISTEMA DE DETECCIÓN DE INTRUSIONES

Analisis de productos comerciales

Dragon - Enterasys Networks

El IDS de Enterasys Networks, Dragon [7], toma información sobre actividades sospechosas de un sensor denominado Dragon Sensor y de un módulo llamado Dragon Squire que se encarga de monitorizar los logs de los firewalls y otros sistemas. Esta información es enviada a un producto denominado Dragon Server para posteriores análisis y correlaciones. Cada componente tiene ventajas que compensan con debilidades de otro, por ejemplo, el sensor Dragon Sensor es incapaz de interpretar tráfico codificado de una sesión web SSL, pero el producto Dragon Squire es capaz de recocer los logs del servidor web y pasárselos a la máquina de análisis. Veamos un poco más en detalle cada uno de estos componentes.

Dragon Sensor - Network IDS

El sensor de Dragon monitoriza una red en busca de evidencias de actividades hostiles. Cuando éstas ocurren, envía informes junto con un registro de análisis forense al servidor Dragon, el cual lo analiza y lo almacena durante largo tiempo.

Características del Sensor: Detección de actividades sospechosas tanto mediante firmas como mediante técnicas basadas en anomalías.

Decodificación robusta a nivel de aplicación: el censor tiene un conocimiento avanzado de los protocolos a nivel de aplicación, evitando muchos falseos que los atacantes utilizan para burlar IDSs, como por ejemplo:

En HTTP nos podemos referir al fichero "SECRET.TXT" por "SECRET%2eTXT". Si la firma solo busca la primera cadena, será incapaz de detectar un acceso a ese fichero si el atacante utiliza caracteres %.

Espacio en blanco y borrado de caracteres en Telnet y FTP.

Codificación SNMP null-byte.

Otros.

Incorporación de filtros para disminuir los falsos positivos.

Monitorización de redes de alta velocidad (100 Mb/s)

Técnicas para evitar falseos anti-NIDS incluyen técnicas para evitar inserción y evasión, tales como:

Ignorar paquetes con un TTL pequeño.

Ignorar paquetes mayores que la MTU de la red con el bit DF activado.

Otros.

Honeypots virtuales: el sensor incluye una variedad de características que permiten al administrador del IDS colocar numerosas trampas para escáneres de red y atacantes. Por ejemplo, el censor tiene la habilidad de etiquetar direcciones IP individuales o bloques CIDR y capturar todo el tráfico dirigido a ellos. Si este rango de IPs no corresponde a ningún host de nuestra red, seguramente serán intentos de ataques y escaneos.

Los sistemas operativos soportados por el Sensor son:

- Linux
- Solaris (Sparc y x86)
- HP-UX
- FreeBSD
- OpenBSD

El censor incluye dos tarjetas de red a 100Mb/s y una única interfaz Gigabit Ethemet. Está diseñado para agregar tráfico desde múltiples enlaces T3 o E3 o para núcleos Gigabit que requieran de monitorización IDS. Provee más de 1300 firmas. Estas firmas pueden ser elaboradas por el usuario final, aunque debido a la flexibilidad y potencia de su sintaxis la labor es complicada y requiere de cursos de entrenamiento.

Dragon Squire

Dragon Squire se encarga de monitorizar los logs de sistemas de producción y firewalls, en busca de evidencias de actividad maliciosa o sospechosa. Está basado en firmas al igual que Dragon Sensor, y a diferencia de otros IDS's basados en host, puede monitorizar los logs de la aplicaciones que corren en el host, tales como servidores web, mail o FTP.

Servidor Dragon - Consolas de análisis

Muchos de los IDS comerciales están muy limitados en cuanto a los análisis que pueden realizar sobre los datos que capturan. Muchas veces se incorpora una tercera herramienta que ofrece información básica sumariada y poco más.

El servidor Dragon intenta ofrecer herramientas más similares a la forma en la que los analistas de IDSs hacen su trabajo. Incluye tres aplicaciones web para análisis que soportan análisis de eventos en tiempo real, correlación de tendencias e inspección detallada de cada evento y su información asociada.

Normalmente, los administradores de los IDSs no se sientan delante de sus monitores en espera de alarmas, sino que configuran sus IDSs para enviar alertas al centro de operaciones de red. Si se detecta una alerta, un administrador puede usar varios interfaces web distintos para analizar tales eventos. También se incluye una interfaz de línea de comando, puesto que muchos administradores encuentran este tipo de interfaces más eficiente. Dragon incluye un completo conjunto de herramientas de línea de comandos para facilitar el análisis de eventos sin el uso de un explorador.

Consola de análisis forense

La consola de análisis forense es un conjunto de aplicaciones que procesan datos de eventos usando herramientas de línea de comandos y nos permiten ver a bajo nivel información sobre los paquetes que hicieron saltar las alarmas. También es posible la visualización mediante un interfaz gráfico basado en web, que nos permite almacenar eventos y ordenarlos en base a parámetros relevantes.

Consola en tiempo real

Proporciona una aplicación de alta velocidad para analizar varios millones de eventos con la misma funcionalidad que nos proporciona una página web (ver figura 1.10). Se basa en el programa "rts" o "real-time shell", que lee nuevos eventos de los sensores y los almacena en un buffer circular. Almacenar un millón de eventos en el anillo solo toma unos 24MB de memoria, por lo que dedicar un servidor para correr solo la consola en tiempo real puede proporcionar una capacidad de varios millones de eventos en memoria.

La aplicación web que envuelve al binario "rts" proporciona una funcionalidad muy similar a la consola de análisis forense, pero, adicionalmente, muestra gráficas de las estadísticas en el tráfico. Casi todas las herramientas en la consola de tiempo real incluyen una opción en vivo que permite el refresco automático cada 1,5 o 15 minutos.

Consola de correlaciones

La consola de correlaciones de Dragon se utiliza para responder consultas correladas. Para ello se utilizan bases de datos SQL, entre ellas MySQL, Oracle, Sybase o MSSQL. Utiliza consultas SQL para buscar eventos de forma eficiente con un criterio de búsqueda complicado. Para cada consulta se utiliza un sofisticado applet para mostrar la ocurrencia de los resultados con más positivos en un periodo de tiempo seleccionado de antemano.

NetRanger - Cisco Systems

El sistema de detección de intrusos de Cisco, conocido formalmente por Cisco NetRanger [5], es una solución para detectar, prevenir y reaccionar contra actividades no autorizadas a través de la red.

Internet Security Systems – RealSecure ®

RealSecure ® Network Sensor

RealSecure ® proporciona detección, prevención y respuestas a ataques y abusos originados en cualquier punto de la red. Entre las respuestas automáticas a actividades no autorizadas se incluyen el almacenar los eventos en una base de datos, bloquear una conexión, enviar un mail, suspender o deshabilitar una cuenta en un host o crear una alerta definida por el usuario.

El sensor de red rápidamente se ajusta a diferentes necesidades de red, incluyendo alertas específicas por usuario, sintonización de firmas de ataques y creación de firmas definidas por el usuario. Las firmas son actualizables automáticamente mediante la aplicación X-Press Update. El sensor de red puede ser actualizado de una versión a otra posterior sin problema, asegurando así la última versión del producto.

Todos los sensores son centralmente gestionados por la consola RealSecure ® SiteProtector, incluyen do la instalación automática, desarrollo y actualizaciones. RealSecure ® Sentry proporciona detección de intrusiones en tiempo real. Tiene mecanismos de respuesta a comportamientos sospechosos en un segmento de red. Los drivers de captura de paquetes a alta velocidad funcionan sin causar el más mínimo impacto en la red. Están disponibles en full duplex, multipuerto y Gigabit.
RealSecure ® Guard es un filtro que protege segmentos de red, incluyendo sistemas de producción críticos o conexiones. El tráfico que atraviesa el sistema Guard, es analizado en tiempo real en búsqueda de evidencia de ataques o abusos. Si se detecta un comportamiento anormal, Guard bloquea el ataque e impide que pase a través del otro interfaz.