Sistemas de Detección de Intrusos (Ids), Seguridad en Internet

M. en C. Mauricio Olguín Carbajal
M. en C. Israel Rivera Zárate
Ing. Patricia Pérez Romero
Profesores del CIDETEC-IPN

El aumento y la gravedad de los ataques en la Internet, hacen que los sistemas de detección de intrusos sean una parte indispensable de la seguridad en las empresas, por lo que se tienen buenas razones comerciales y legales para establecer políticas de seguridad sólidas; por esta razón, es esencial instalar un Sistema de Detección de Intrusos (IDS).

Los sistemas de detección de intrusos no son precisamente nuevos, el primer trabajo sobre esta materia data de 1980; no obstante, este es uno de los campos con mayor auge desde hace algunos años dentro de la seguridad informática. La capacidad para detectar y responder ante los intentos de ataque contra los sistemas es realmente interesante; durante este tiempo, cientos de investigadores de todo el mundo han desarrollado, con mayor o menor éxito, sistemas de detección de todo tipo, desde simples procesadores de archivos históricos (*logs),* hasta complejos sistemas distribuidos, especialmente vigentes con el auge de las redes de computadoras en los últimos años.

Introducción

Se considera a un intruso como cualquier persona que intente interrumpir o hacer mal uso del sistema; los sistemas informáticos se apoyan en los Sistemas de Detección de Intrusos, para prepararse del mal manejo y del uso indebido de la información de una organización. Esta meta se logra recopilando la información de una gran variedad de fuentes del sistema y de la red, analizando la información que contribuye a los síntomas de los problemas de seguridad de la misma, y permitiendo que el usuario especifique las respuestas en tiempo real a las violaciones. Es muy importante que, ante estos posibles ataques, se pueda responder a ellos en tiempo real.

Desarrollo

En general hay 2 tipos de intrusiones

Intrusiones para mal uso.- Son ataques en puntos débiles conocidos que pueden ser detectados haciendo un análisis y revisión en la información de auditoría y reportes del sistema; por ejemplo, un intento de crear un archivo inválido, puede ser descubierto examinando los mensajes en los archivos históricos (bitácoras) que son resultado de las llamadas al sistema.

Intrusiones anómalas.- Se basa en la observación de desviaciones de los patrones de uso normales del sistema. Estas intrusiones son difíciles de detectar, ya que no hay patrones fijos y permanentes; se pueden usar métricas que calculan parámetros del sistema disponibles, tales como el promedio de carga del CPU, número de conexiones de la red por minuto, número de procesos por usuario y cualquier otro tipo de medida que describa un cierto consumo de recursos en un periodo definido; el inconveniente es que si estas métricas cambian, porque así lo exige el sistema por sobrecarga de trabajo, se interpretará erróneamente como una intrusión.

Los objetivos que debe tener un sistema de detección de intrusos son los siguientes:

1. Vigilar y analizar la actividad de los usuarios y del sistema.
2. Revisar las configuraciones del sistema y de las vulnerabilidades.
3. Evaluar la integridad de los archivos críticos del sistema.
4. Reconocimiento de los modelos de la actividad que reflejan ataques conocidos.
5. Análisis estadístico para los modelos anormales de la actividad, aunque esto no siempre es exitoso, debido a que los promedios pueden cambiar.

6. Búsqueda de rastros de intervención al sistema operativo, con el reconocimiento de las violaciones de la actividad del usuario respecto a la política establecida.

7. Vigilar el cumplimiento de políticas y procedimientos de seguridad en la organización.

La meta de un IDS es proporcionar una indicación de un ataque potencial o de uno verdadero; un ataque o una intrusión son acontecimientos transitorios, mientras que una vulnerabilidad representa una exposición, que lleva el potencial para un ataque o una intrusión. La diferencia entre un ataque y una vulnerabilidad es que un ataque existe en un momento determinado, mientras que una vulnerabilidad existe independientemente de la época de la observación. Esto nos conduce a categorizar varios tipos de IDS:

* IDS basado en red.
* IDS basado en anfitrión (host).
* IDS híbridos.
* Inspector de la Integridad del Archivo.
* Explorador de la vulnerabilidad de la red.
* Explorador de la vulnerabilidad del host.

Los tres primeros puntos son tipos de IDS, mientras que los tres siguientes son herramientas de detección de vulnerabilidad.

Los sistemas basados en red actúan como detectores, es decir, ellos observan el tráfico en las capas del TCP/IP y buscan modelos conocidos de ataque, como los que generalmente realizan los hackers; la mayoría de los sistemas basados en red pueden buscar solamente los modelos de abuso que se asemejan al estilo de estos ataques, y esos perfiles están cambiando constantemente. Los sistemas basados en red también son propensos a los positivos falsos; por ejemplo, si el servidor Web tiene sobrecarga de trabajo y no puede manejar todas las peticiones de conexión, los IDS quizá pueden detectar un ataque inexistente. Típicamente, un sistema basado en red no va a buscar otras actividades sospechosas, como podría ser que alguien de su entorno de trabajo intente tener acceso a los datos financieros de la compañía.

Los sistemas basados en anfitrión emplean diversos procedimientos para buscar a los malos usuarios; estos sistemas dependen, generalmente, de los registros del sistema operativo para detectar acontecimientos, y no pueden considerar ataques a la capa de red mientras que estos ocurren. En comparación con los IDS basados en red, estos sistemas obligan a definir lo que se considera como actividades ilícitas, y a traducir la política de la seguridad a reglas del IDS. Los IDS basados en anfitrión se pueden también configurar para buscar tipos específicos de ataques.

Los sistemas relacionados al anfitrión (host) se despliegan de la misma forma que los buscadores de los antivirus o las soluciones de administración de red: se instala algún tipo de agente en todos los servidores y se usa una estación de gestión para generar informes.

Los vendedores observaron las limitaciones que presentan los IDS de red y los basados en anfitrión, y han combinado ambos para mejorar sus capacidades; estos sistemas híbridos reunen las mejores características de los dos en una configuración del sensor del IDS; como ejemplos se tienen Real Secure de Internet Security Systems (ISS) y, CyberCop de Network Associates (NAI).

A continuación se desglosan los errores que puede tener el sistema:

* Los errores positivos falsos conducirán a los usuarios del IDS a no hacer caso de su salida, pues clasifican acciones legítimas como intrusiones. Las ocurrencias de este tipo de error se deben reducir al mínimo; si muchos positivos falsos se generan, los operadores no haran caso de la salida del sistema en un cierto plazo, lo que puede conducir a una intrusión real que es detectada, pero que no es considerada por los usuarios, esto es un ejemplo de lo que se mencionó anteriormente.

* Un error negativo falso ocurre cuando procede una acción, aunque sea una intrusión. Los errores negativos falsos son más serios que los errores positivos falsos, porque dan un sentido engañoso de la seguridad. Permitiendo que todas las acciones procedan, una acción sospechosa no será atraída a la atención del operador. El IDS ahora es un defecto, pues la seguridad del sistema es menor que la anterior a que el IDS fuera instalado.

* Los errores de cambio son más complejos: un intruso podría utilizar conocimientos sobre los mecanismos internos de un IDS para alterar su operación, permitiendo posiblemente que el comportamiento anómalo proceda; el intruso podría entonces violar las necesidades operacionales de la seguridad del sistema. Esto se puede descubrir por un operador humano que examina los registros del detector de la intrusión, pero parecería que el IDS aún trabaja correctamente.

Otro aspecto a considerar al adquirir un sistema de detección de intrusos es que a veces se invierte en un sistema de detección de intrusos difícil de soportar, ya que reporta demasiados falsos positivos, y no puede

responder con la velocidad de la red. Para reducir las posibilidades de que esto suceda, las empresas deben tomar en cuenta los siguientes criterios al evaluar un sistema de detección de intrusos IDS:

- Un Sistema de detección de intrusos debe ir más allá de la simple notificación, proporcionando respuestas automatizadas, basadas en políticas para proteger los sistemas y ofreciendo tiempo y tranquilidad al personal de seguridad. Cuando es necesario localizar el origen de un ataque (frecuentemente se ataca con una dirección falsa), el enfoque tradicional ha sido interrogar manualmente a los enrutadores y encontrar el flujo relevante de los datos; este es un ejercicio agotador que puede llevar muchas horas o días, incluso para un ingeniero de redes experimentado. Una empresa debe a cambio escoger un IDS que pueda rastrear los ataques rápida y automáticamente, incluso aquellos con referencias falsas, o que se reflejan de regreso al punto de ingreso de la red. Esto permitirá a la empresa reaccionar rápida y eficientemente para bloquear los ataques de negación de servicio que pueden afectar la disponibilidad del ancho de banda y del servicio.

- Un sistema IDS debe manejar los escenarios de instalación más grandes y exigentes, incluyendo el monitoreo de los múltiples segmentos de la red.

- Un sistema IDS debe tener un motor de análisis y correlación que analice los numerosos eventos que suceden en la red y los evalúe en su contexto. El tiempo y el conocimiento son críticos para lanzar una respuesta rápida y efectiva a los ataques contra los activos empresariales de misión crítica en el momento en que se produzcan. La acumulación de eventos en tiempo real, la correlación y el análisis pueden reducir dramáticamente el esfuerzo que tradicionalmente se exige del personal de seguridad para darle tiempo a que realice un trabajo de investigación, en lugar de pasar horas examinando los registros de eventos no correlacionados.

- Un sistema IDS debe recoger los datos importantes de detección directamente de los conmutadores de redes, lo que reduce la cantidad de sensores que se necesita instalar y administrar en toda la red, a fin de reducir el Costo Total de Propiedad. Muchas empresas no se dan cuenta de que la ampliación de los sistemas IDS diseñados específicamente para redes conmutadas de alta velocidad cuesta menos que la de los sistemas tradicionales. Una instalación tradicional requiere de un sensor para cada segmento de la red, además del costo del hardware, software y de la administración del sistema.

Cuando una compañía necesita expandirse para tener cobertura de red total, los costos asociados al financiamiento de los sensores, hardware, software y administración del sistema serán comparables a los costos de aquellos componentes de la instalación inicial; por el contrario, un sistema IDS diseñado para funcionar en redes conmutadas de alta velocidad, permite una cobertura máxima sin el costo agregado de la administración del sistema.

Un sistema IDS con la herramienta de localización puede compararse a un grupo de cámaras de seguridad almacenadas convenientemente; sin embargo, a diferencia de dichas cámaras, el sistema IDS debe tener la inteligencia para saber que ha ocurrido un incidente, para continuar recogiendo datos y alertar al administrador del sistema. Con este tipo de sistema, los ahorros empresariales tan sólo en concepto de soporte, instalación y mantenimiento pueden ser significativos.

Conclusiones

Este articulo presenta de manera breve lo que es un IDS, y algunos criterios para su elección, así como una recomendación a las empresas que aún no han invertido en un software de detección de intrusos para considerar la adquisición de uno; aplazar esta inversión supone para la empresa un riesgo no únicamente de modificación, destrucción y robo de la información, sino de ser objeto de demandas legales. El sistema IDS que la empresa adopte en última instancia, debe proporcionar un método muy bien coordinado para administrar los asuntos de seguridad, desde la identificación de robos en la red y obtención de información adicional solicitada, hasta responder rápidamente y tomar las medidas adecuadas.

Referencias

[1] http://www.infosecuritymag.com/newsletter/

[2] http://www.guardiacivil.org/kio/seg/sld001.htm

[3] http://www.idsdetection.com/

[4] www.icsa.net

[5] http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml