Evaluación de PreludeIDS como herramienta de gestión de información y eventos relativos a seguridad

Leonardo de- Matteis* Javier Echaiz Jorge R. Ardenghi

Laboratorio de Investigación en Sistemas Distribuidos
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
Bahía Blanca - Buenos Aires - Argentina
e-mail: {ldm,je,jra}@cs.uns.edu.ar

Resumen

Dentro de los aspectos que abarca la seguridad en sistemas se cuenta el acceso y uso de redes de datos para interconectar diversos centros de datos, redes de computadoras y equipos móviles.

Por otra parte, la interoperatibilidad a través de Internet involucra permanentes riesgos y desafíos a la seguridad de las organizaciones. Por ello están siempre bajo riesgo los activos físicos (infraestructura computacional) y los datos (información contenida). Ambos activos deben resguardarse a través de los mecanismos que provee la seguridad en sistemas, en sus diversos tópicos (redes de computadoras, sistemas operativos, bases de datos, etc.), pero debe entenderse, entonces, que contar con herramientas que permitan evaluar los eventos que se producen resulta imperativo.

Esta línea de investigación pretende evaluar el sistema PreludeIDS, seleccionado porque permite alcanzar los objetivos planteados obteniendo la información necesaria a partir de los registros y archivos generados por sistemas de uso extendido en el ámbito de la seguridad, por ejemplo, *Snort*, *AuditD*, *samhain*, *Tripwire*, *OSSEC*, entre otros, además de presentar compatibilidad para analizar varios tipos de *logs*.

Palabras clave: Seguridad en sistemas, seguridad en redes, detección de intrusos, automatización, IDS, SIEM/SEM/SIM, PreludeIDS.

*Este trabajo forma parte de los avances de mi tesis de maestría sobre *Seguridad en redes y argumentación.*

Contexto

El presente trabajo se realiza en el ámbito del Laboratorio de Investigación y Desarrollo en Sistema Distribuidos que funciona en el Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur. Se inscribe en el marco del Proyecto de Investigación "Automatización de la detección de intrusos a partir de políticas de seguridad", dirigido por el Mg. Javier Echaiz y financiado por la Secretaría General de Ciencia y Tecnología de la UNS (24/ZN14).

Introducción

Dada la interoperatibilidad que supone en la actualidad el recurso constante y ubicuo a Internet para organizaciones de todo tipo, resulta imperativo que las mismas cuenten con políticas que determinen la obligatoriedad en el uso de herramientas que les permitan:

- prevenir y evadir ataques;
- informar cuándo se producen y, en los mejores de los casos,
- reaccionar proactivamente durante dichos sucesos.

En este sentido, las organizaciones deberían generar procedimientos para reaccionar automáticamente mediante los sistemas informáticos adecuados ante los mismos (por ejemplo, a través de una interacción efectiva entre sistemas de detección de intrusos [4, 2] y *firewalls*). Pero, además, se deberían determinar y establecer por escrito políticas

que especifiquen qué medidas y pasos de acción deben tomarse y seguirse cuando se produzcan en el futuro ataques de la misma naturaleza. De manera general, esto significa establecer, en primer lugar, los mecanismos de análisis para tomar acciones y, en segundo lugar, implementar las medidas concretas que permitan:

- evadir los ataques;
- prevenir nuevos eventos en el futuro;
- impedir efectos no deseados.

Los daños colaterales que evitará este tipo de planificación organizacional tienen una importancia radical para la eficiencia de las operaciones de cualquier organismo. Dichos daños son la pérdida o, peor aún, el robo de datos; los sistemas que dejan de funcionar y/o la paralización momentánea de los procesos internos, con los consecuentes daños y perjuicios económicos.

Los activos deben resguardarse a través de los mecanismos que provee la seguridad en sistemas, con herramientas que permitan:

- investigar los eventos que se generan a partir de los ataques e intentos de vulnerar la seguridad, reaccionando de manera proactiva al momento de producirse;
- producir reportes, para que los referentes encargados de la seguridad los analicen con mayor facilidad y claridad, para así
- poder decidir e implementar acciones futuras de protección.

La línea de investigación pretende evaluar el sistema PreludeIDS [9], seleccionado porque permite alcanzar los objetivos planteados obteniendo la información necesaria a partir de los registros y archivos generados por sistemas de uso extendido en el ámbito de la seguridad, por ejemplo *Snort*, *AuditD*, *samhain*, *Tripwire*, *OSSEC*, entre otros, además de presentar compatibilidad para analizar varios tipos de *logs*.

Después de esta evaluación, se intentará extender PreludeIDS para su utilización relacionada con técnicas de razonamiento argumentativo. Es decir, se tratará de ampliar el uso de la base de datos para incorporar dichas técnicas de razonamiento a fin de mejorar el análisis de datos a través de patrones predeterminados y estadísticas típicas de los sistemas de gestión de información y eventos de seguridad.

Antecedentes

Hoy en día se están desarrollando nuevas aplicaciones que permiten centralizar el almacenamiento y la interpretación de eventos (desde diversas bitácoras/*logs*) que provienen de los diferentes sistemas en uso dentro de una organización. Dichas aplicaciones se denominan SIEM, del inglés *Security information and event manager*. Ahora bien, se hace necesario realizar algunas consideraciones previas respecto de la terminología y los acrónimos que se emplean en esta área [5]. Si bien las siglas SEM, SIM y SIEM —que será la que emplearemos en este trabajo— se han utilizado como equivalentes, aluden a sistemas con diferentes características y capacidades:

- SIM (*Security Information Management*): hasta hace un par de años, esta sigla era la que predominaba haciendo referencia al almacenamiento de datos durante largo plazo (*logs*, eventos, etc.) así como al análisis y reporte de los datos registrados.
- SEM (*Security Event Management*): este tipo de gestión es relativamente novedosa y está en desarrollo. Se utilizan estos sistemas para monitorear en tiempo real y correlacionar diversos eventos, posibilitan generar notificaciones y obtener reportes.
- SIEM (*Security Information Event Management*): este tipo de sistemas permite obtener, analizar y presentar información obtenida de diversos dispositivos y aplicaciones. Cuentan con herramientas de administración y manipulación de políticas, permiten auditar diversos tipos de sucesos, filtrar datos para investigar incidentes y monitorerar la utilización de privilegios.

En este tipo de sistemas, las características mencionadas permiten dar soporte y efectividad a las tareas de seguridad en el ámbito de la infraestructura computacional de la organización.

Estos sistemas poseen, en síntesis, las siguientes capacidades:

- recolección de datos y eventos;
- agregación y correlación de los mismos en tiempo real [3];

- interfaces hombre-máquina adecuada para visualizar, monitorear y administrar los eventos;
- respuesta automática para aquellos eventos que tienen relación directa con la seguridad.

Por otra parte, los sistemas SIM se caracterizan principalmente por permitir mayor análisis histórico de los datos y eventos almacenados en los mismos. Así como también incluyen la posibilidad generar diversos tipos de reportes. Estos sistemas posibilitan también el aplicar técnicas de correlación sobre los datos y eventos, pero no en tiempo real. Se cuenta en ellos con un repositorio para los sucesos (*logs*) y, por lo general, algún mecanismo flexible de consulta que permite obtener reportes diversos.

En ambos tipos de sistemas, se dispone de la posibilidad de aplicar filtros, ya que es común hoy en día la gran cantidad de datos que se obtienen, generan y almacenan, por la naturaleza propia de las actividades de los mismos (entre ellos: IDS (*Intrusion Detection System)*, *firewalls*, *logs* de aplicaciones y equimiento de diverso tipo).

Caracterización de sistemas SIEM

Ahora bien, como una instancia mejorada y ampliada, los sistemas SIEM se caracterizan por combinar las características de los sistemas de tipo SEM y SIM, de ahí el acrónico que los representa actualmente.

Una de las principales características, entonces, es que estos sistemas poseen tecnologías adecuadas para correlacionar diversos tipos de datos de diversas fuentes de origen. La posibilidad de contar con una correlación es aquella capacidad de establecer y formar relaciones entre los diversos datos (*logs*, sucesos, etc.) de diferentes dispositivos (ya sean de *software* o *hardware*). Dichas correlaciones se basan en características tales como: origen, destino, protocolo o tipo de evento. Además, las correlaciones en sí mismas permiten filtrar información duplicada y/o redundante para así poder eliminar aquellos sucesos que entorpecen un análisis adecuado. De esta manera, los administradores de la infraestructura de la organización pueden manipular mayor cantidad de sucesos más rápidamente, con mayor efectividad, haciendo uso de información correcta y suficiente para así poder encarar acciones adecuadas y establecer nuevas políticas a futuro (según el tipo de suceso). Cabe destacar que las correlaciones se establecen, básicamente, mediante dos mecanismos de análisis de los datos: mediante reglas preestablecidas (que analizan los patrones de los sucesos) o bien en base al análisis estadístico de los mismos. Y, por supuesto, al establecer correlaciones se debe tener en cuenta el período de ocurrencia de los sucesos. El tiempo en este tipo de sistemas es un factor fundamental para el análisis y las acciones subsiguientes que se deberán tomar.

Las características más específicas de los SIEM pueden sintetizarse de la siguiente manera:

- Agregación de datos: cuentan con la posibilidad de adquirir información de diversas fuentes: redes, servidores, bases de datos, aplicaciones, etc. Con la capacidad para consolidar los datos obtenidos y no perder sucesos importantes.
- Correlación: a través de diferentes mecanismos, se efectúa una búsqueda sobre atributos comunes y se establecen relaciones entre diversos sucesos, para poder unirlos y verlos como un único evento aunque los datos provengan de diferentes fuentes.
- Alertas: análisis automático y generación de alertas para notificar a los administradores de los sucesos más relevantes.
- Capacidad forense: la posibilidad de utilizar herramientas de investigación y análisis para poder investigar las alertas, determinar el origen de los sucesos y así organizar las acciones preventivas.
- Tablero de instrumentos: estas herramientas toman los datos de los distintos sucesos y posibilitan visualizarlos a través de diferentes mecanismos gráficos, adecuados para la interacción de los usuarios del sistema, de tal forma que éstos puedan identificar a simple vista patrones diversos de funcionamiento del sistema y alertas recientes.
- Cumplimiento: son utilizadas para automatizar la recolección de datos que satisfacen los requisitos/políticas de seguridad para la organización. Gracias a ellos, se pueden producir reportes que se adapten a los procesos de auditoría internos.

- Archivo: estos sistemas permiten almacenar por largo tiempo un gran volumen de datos para facilitar luego las tareas de correlación propias de los mismos durante su tiempo de vida.

Líneas de investigación y desarrollo

La aplicación que nos proponemos poner en producción, se denomina PreludeIDS. Su documentación oficial lo presenta tanto como un SIM, como en calidad de SIEM. Como hemos visto, un sistema SIEM incluye las características y funcionalidades de un SIM.

Por lo tanto, según sus desarrolladores, PreludeIDS tiene como principales funcionalidades la recolección, normalización, ordenamiento, agregación, correlación y generación de reportes para los sucesos que procesa.

PreludeIDS

De acuerdo con las características enunciadas para los sistemas SIEM, entonces, PreludeIDS es capaz de procesar diversos tipos de registro de datos (*logs*, archivos de eventos, datos de *syslog*, etc.). Para ello, PreludeIDS hace uso de variadas aplicaciones que mejoran la adquisición de información referente a los sucesos (Snort, samhain, OSSEC, AuditD, etc.).

Esta aplicación se caracteriza, además, por contar con un único formato denominado "Intrusion Detection Message Exchange Format" (IDMEF), que es un estándar internacional creado por la IEFT (*Internet Engineering Task Force*) junto con el equipo de desarrollo de PreludeIDS para permitir la interacción de las diversas herramientas globalmente disponibles en la actualidad relacionadas con la seguridad en sistemas y gestión de redes.

Como corolario de estas características, esta aplicación permite:

- evitar fallas de seguridad y pérdida de datos;
- implementar políticas de seguridad;
- recibir advertencias de amenazas y sucesos sospechosos;
- relacionar sucesos y consecuencias de forma automática;
- determinar situaciones de baja eficiencia y sus causas;
- monitorear la actividad sobre redes;
- contar con pruebas para mejores prácticas de auditorías.

Componentes

Los componentes que conforman el sistema PreludeIDS se dividen de las siguiente manera:

- Una interface gráfica (Prewikka), que actúa como consola para el análisis de los datos que manipula el sistema.
- Prelude manager: servidor que acepta las conexiones de los sensores distribuidos, que proveen de datos sobre sucesos al sistema.
- Libprelude: API para la comunicación con los subsistemas que componen PreludeIDS.
- LibpreludeDB: capa de abstracción que permite a los desarrolladores utilizar la base de datos IDMEF del sistema PreludeIDS sin preocuparse del tipo de base de datos y del lenguaje SQL.
- Prelude-LML: un analizador de logs, que permite recolectar y analizar la información recibida desde diferentes dispositivos o sistemas.
- Prelude-Correlator: es el motor que permite establecer las correlaciones entre los datos almacenados, para simplificar así el análisis de los sucesos, en forma rápida y precisa. (Distribuido bajo licencia GPL).
- Mail reporting plugin: permite enviar notificaciones automáticas a diferentes usuarios del sistema.
- Sensores: PreludeIDS utiliza sensores de uso generalizado hoy en día, de sabida calidad y estabilidad, entre ellos podemos citar: Snort, Auditd, OSSEC, Samhain, Nepenthes, etc.

Objetivos

Esta línea de investigación se dividirá en dos etapas. En la primera de ellas, a partir de la instalación y análisis que permitirá la puesta en funcionamiento del sistema PreludeIDS en el equipamiento adecuado previsto en el plan de trabajo de

maestría, se espera constatar las ventajas y desventajas del mismo para las organizaciones que requieran su empleo en la gestión de la seguridad de sus sistemas.

Entre las ventajas que se espera observar de acuerdo a lo investigado, se cuentan:

- significativa reducción de la sobrecarga de información para la toma de decisiones;
- disminución de falsos positivos, es decir, alertas sobre ataques no reales;
- reducción paralela de falsos negativos, esto es, la falta de acción ante sucesos no identificados como ataques;
- la posibilidad de correlacionar diferentes eventos en la misma cadena de sucesos;
- en estrecha relación con el punto anterior, la consolidación de sucesos detectados por diferentes sistemas como un solo evento.

La implementación de sistemas tipo SIEM demanda una inversión importante en tiempo y dinero que se vincula fuertemente con los sistemas de administración de redes. Los volúmenes de datos a analizar en tiempo real derivados de las alertas demandan, además, considerable capacidad de almacenamiento y *performance* para su análisis. En las redes de gran escala, se hacen necesarios anchos de banda considerables. Además, debe acompañarse la implementación con la constante detección de fallas de comunicación en los enlaces.

Cabe destacar, por último, que un SIEM es naturalmente un sistema distribuido y, como tal, está sujeto a los problemas propios de este tipo de sistemas, en cuanto a pérdida de conectividad o disponibilidad de algún equipo integrante del sistema. Por lo tanto, resulta crítico no perder eventos y analizar cuál será el nivel de redundancia será necesario en aspectos tales como equipos y enlaces.

En una segunda etapa de desarrollo, se tratará de incorporar modificaciones al sistema PreludeIDS que permitan trabajar con técnicas de razonamiento argumentativo, en particular manipulando la base de datos de formato IDMEF con el objetivo de generar análisis complementarios que mejoren la identificación de sucesos.

Formación de recursos humanos

Esta nueva línea de investigación dentro del proyecto citado, involucra un desarrollo de tesis de maestría en marcha. Además, se considera un contexto adecuado para desarrollar proyectos integradores de fin de carrera con alta significación experimental.

Referencias

[1] Michael Attig and John Lockwood. Sift: Snort intrusion filter for tcp, 2005.

[2] Stefan Axelsson. Intrusion detection systems: A survey and taxonomy. Technical report, 2000.

[3] Frederic Cuppens, Fabien Autrel, Alexandre Miege, Salem Benferhat, and Re Mi Ege. Correlation in an intrusion detection process, 2002.

[4] Martin Roesch and Stanford Telecommunications. Snort - lightweight intrusion detection for networks. pages 229–238, 1999.

[5] David Swift. A practical application of sim/sem/siem: Automating threat identification. Technical report, The SANS Institute, 2006.

[6] Jeffrey Undercoffer, Anupam Joshi, and John Pinkston. Modeling computer attacks: An ontology for intrusion detection. In *In: 6th International Symposium on Recent Advances in Intrusion Detection*, pages 113–135. Springer, 2003.

[7] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel, and Richard A. Kemmerer. A comprehensive approach to intrusion detection alert correlation. *IEEE Transactions on Dependable and Secure Computing*, 1:146–169, 2004.

[8] David Wagner and Drew Dean. Intrusion detection via static analysis, 2001.

[9] Krzysztof Zaraska. Prelude IDS: current state and development perspectives, 2003.