Revista Educación en Ingeniería
ISSN 1900-8260
Diciembre de 2008 • N°. 6 • Pp 29-37 • Publicado en línea por la Asociación Colombiana de Facultades de Ingeniería -ACOFI- www.acofi.edu.co
Enviado: 24/10/2008 • Aprobado: 31/10/2008

IMPLEMENTACIÓN Y MEJORA DE LA CONSOLA DE SEGURIDAD INFORMÁTICA OSSIM: UNA EXPERIENCIA DE COLABORACIÓN UNIVERSIDAD-EMPRESA

Juan Manuel Madrid Molina, Luis Eduardo Múnera Salazar, Carlos Andrey Montoya González, Juan David Osorio Betancur, Luis Ernesto Cárdenas, Rodrigo Bedoya, Cristian Latorre
Universidad ICESI, Santiago de Cali (Colombia)

Resumen

La consola de seguridad es una de las herramientas más usadas para la gestión de la seguridad informática en las organizaciones. Este artículo resume el trabajo efectuado por el equipo de investigación para integrar una serie de mejoras a la consola de seguridad informática OSSIM, con el fin de cubrir las necesidades del entorno colombiano. Dichas mejoras incluyen la interconexión con dispositivos de seguridad física, la implementación de un módulo de creación automática de directivas de correlación para el motor de la herramienta, y la mejora significativa de la confiabilidad de captura de información en redes con alto tráfico.

Palabras clave: Seguridad informática, seguridad física, consolas de seguridad, OSSIM, correlación de alertas.

Abstract

Security management consoles are today among the most widely deployed tools for information security management in the enterprise. This article summarizes the work done by our research group, in order to implement a series of improvements to the OSSIM security console, aiming to fulfill the Colombian market needs. The improvements include an interface with physical security devices, the creation of a software module for automatic creation of correlation rules, and a significant enhancement of information capture reliability in highly congested networks.

Key words: Information security, physical security, security consoles, OSSIM, alert correlation.

Introducción

La gestión de la seguridad informática se ha convertido en una necesidad para las organizaciones de hoy debido a exigencias legales (Unión Europea, 2000; Congreso Estados Unidos, 2002) y de cumplimiento con estándares internacionales (ISO 17799, 2005; ISO 27001, 2005).

Una de las herramientas más útiles en dicha labor es la consola de gestión que recoge información de los diferentes equipos y redes que conforman la

plataforma informática de la organización, con el fin de detectar configuraciones y/o eventos que podrían considerarse como una amenaza o una evidencia de ataque informático, y de esa manera poder reaccionar oportunamente y mantener la información en un estado seguro. La consola de gestión también permite obtener estadísticas e informes acerca del estado de seguridad de los sistemas de la organización, y para verificar el cumplimiento de indicadores de gestión.

Una de las consolas de gestión de código abierto más populares en la actualidad es OSSIM (Open System Security Information Management, OSSIM, 2008). Esta consola, además de recolectar y uniformizar los eventos de los diferentes sistemas, correlaciona aquellos que ocurren en el sistema bajo análisis, con el fin de minimizar el número de alarmas que el administrador recibe y eliminar falsos positivos.

Este artículo describe el trabajo realizado por el equipo investigador para mejorar la funcionalidad de la consola OSSIM. Particularmente, se reseñan el desarrollo de interfaces para capturar información desde dispositivos de seguridad física, la creación de un módulo de software para creación automática de directivas de correlación, y la mejora de la confiabilidad de la captura de datos en redes con alto tráfico. Primero, se presenta un panorama de la seguridad informática y la problemática que es solucionada por las consolas de seguridad. Luego se presenta un resumen de la arquitectura de la consola OSSIM. Seguidamente se exponen las adaptaciones y mejoras que se implementaron sobre la consola, y se cierra con un apartado de conclusiones.

Problemática de Gestión de la Seguridad Informática

Para que un sistema informático se considere como seguro debe cumplir con cuatro premisas básicas (Carracedo, 2004):

- La información que contiene debe ser *confidencial*, es decir, no debe poder ser consultada por terceros que no deberían tener en principio acceso a ella.
- De igual manera, dicha información debe conservar su *integridad,* es decir no dañarse o alterarse a medida que se mueve por el sistema.
- El sistema debe ser capaz de *autenticar* a sus usuarios y a la información que recibe, de tal manera que la fuente de la información siempre sea verificable, y que solamente los usuarios autorizados puedan acceder al sistema.
- Por último, el sistema debe estar *disponible* cuando se lo necesite.

Un ataque informático atenta contra una o varias de estas premisas. Como se puede ver, la labor del oficial de seguridad de un sistema informático no es nada fácil, ya que continuamente se pueden presentar ataques que aprovechen vulnerabilidades existentes o nuevas. La seguridad absoluta no existe, porque a medida que se descubren nuevas vulnerabilidades y se solucionan, dichas soluciones pueden introducir otras vulnerabilidades, o el avance de la tecnología hace que sistemas que antes se consideraban como seguros pasen a ser vulnerables, esto debido al descubrimiento de nuevos métodos de ataque.

De otra parte, la legislación de los diferentes países se ha ido actualizando con el fin de castigar el delito informático, pero a la vez exige que las organizaciones dispongan de un nivel adecuado de protección en los sistemas de información (Unión Europea, 2000; Congreso Estados Unidos, 2002). La seguridad de la información también se ha convertido en asunto crítico para procesos de calidad total de las empresas y estrategias de gobierno de tecnologías de información. En todos estos procesos no solamente se exige que existan mecanismos que garanticen la seguridad (ISO 17799, 2005), sino que se requiere cuantificar su impacto mediante el uso de indicadores (ISO 27001, 2005).

Existen diversas herramientas que pueden ayudar al administrador en la tarea de mantener seguro un sistema informático. Dichas herramientas se pueden clasificar en los siguientes grupos:

- *Antivirus*: Se encargan de detectar y eliminar software maligno de un sistema informático. Dependiendo de su funcionalidad, también pueden controlar los diferentes vectores de infección (correo electrónico, medios de almacenamiento removibles, etc.).
- *Detectores de intrusos basados en host* (HIDS, Host-based Intrusion Detection Systems): Este

tipo de software monitorea procesos y archivos críticos del sistema bajo análisis, y reporta cuando se producen cambios no autorizados que puedan considerarse como evidencia de un ataque informático.
- *Detectores de intrusos basados en red* (NIDS, Network-based Intrusion Detection Systems): Los NIDS revisan continuamente los datos que circulan por la red, y avisan cuando observan tráfico que evidencia un ataque o una tentativa de ataque informático.
- *Firewalls*: Un firewall actúa como aislador entre el tráfico de la Internet y el tráfico interno de la red corporativa. Mediante un conjunto de reglas determina qué paquetes pueden pasar o no a través de él, y registra las violaciones a dicha política.
- *Detectores de vulnerabilidades*: Estos programas hacen un análisis detallado de un sistema de cómputo, desde una perspectiva interna o externa, y arrojan como resultado las vulnerabilidades que existen en el sistema operativo y el software instalado.

La abundancia de herramientas, y el hecho de que deban emplearse varias de ellas en conjunto para monitorear los diferentes frentes del sistema informático trae consigo varios problemas graves:

- Falta de uniformidad en el formato de los registros de actividad.
- Exceso de alertas. En sistemas grandes, o con actividad alta, el número de alertas que se genera en un determinado período de tiempo puede exceder la capacidad de trabajo del administrador.
- Manejo de falsos positivos. Dependiendo de la configuración de las herramientas, pueden reportarse como alertas de seguridad eventos que son, en realidad, parte del funcionamiento habitual del sistema.

En un escenario como éste, se hace necesario contar con una herramienta que permita unificar y centralizar la gestión de las alertas de seguridad. Las herramientas de esta naturaleza se denominan consolas de seguridad. A continuación, se hará una breve descripción de OSSIM, que es la consola de seguridad empleada en nuestro proyecto de investigación.

Generalidades y Arquitectura de OSSIM

La plataforma OSSIM (2008) es una consola de seguridad de código abierto, de amplio uso en la actualidad. Tiene la capacidad de consolidar alertas de una gran cantidad de sistemas de seguridad basados en código abierto, y es altamente configurable, de tal manera que permite procesar información de todo tipo de programas y dispositivos de seguridad. La arquitectura de OSSIM es distribuida y comprende cuatro elementos básicos (Casal, 2008):

- *Elementos de captura de información*: Recolectan la información requerida por OSSIM, en los diferentes sitios del sistema informático en donde se desea hacer control. Virtualmente cualquier programa o dispositivo de seguridad informática puede servir como entrada al sistema OSSIM, siempre que sea capaz de generar archivos de bitácora (log) en formato de texto plano. La interfaz se hace escribiendo un archivo de configuración de plugin adecuado. Los plugins así configurados actúan como traductores de alertas, tomando el registro de la alerta en su formato nativo y traduciéndolo al formato estándar empleado por OSSIM. El elemento clave del archivo de configuración de plugin es la *expresión regular* (Ossim Agent, 2008), que define la manera cómo puede encontrarse la información que OSSIM requiere en el archivo de log.

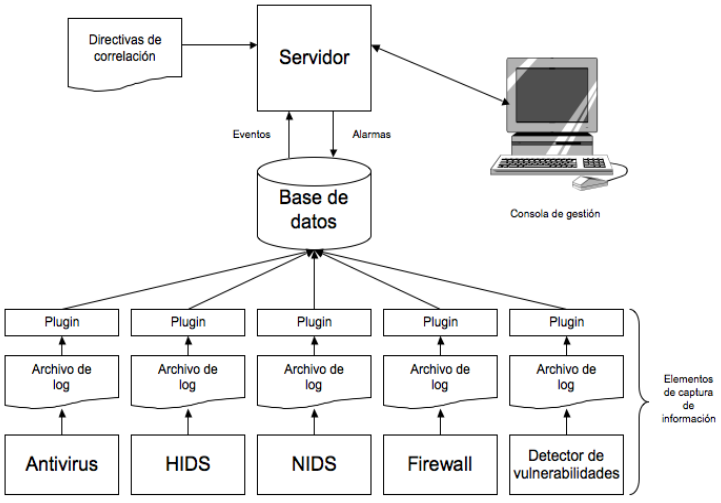

Figura 1. Arquitectura de OSSIM

- *Base de datos*: Almacena todos los eventos recibidos de los diferentes elementos de captura de información, así como las alarmas generadas por el motor de correlación del servidor.
- *Servidor*: El servidor correlaciona los eventos registrados en la base de datos, con el fin de detectar patrones que evidencien una vulnerabilidad en el sistema o un ataque informático, y a la vez actúa como filtro para tratar de eliminar la mayor cantidad posible de falsos positivos. Además, con base en las alarmas que se presenten y en el valor de importancia relativa que el administrador haya asignado a cada uno de los activos informáticos de la empresa, OSSIM es capaz de calcular también el nivel de riesgo informático del negocio.
- *Consola de gestión*: La consola es el front-end gráfico del sistema. Funciona vía web, y permite al administrador del sistema consultar las alarmas, reportes y estadísticas que genera el sistema.

Mejoras Implementadas sobre OSSIM en el Marco del Proyecto de Investigación

En el desarrollo del proyecto de investigación «Adaptación y mejoras al motor de correlación y sensores remotos del sistema OSSIM para un centro de seguridad informática», acometido por la Universidad Icesi y Sistemas TGR, S.A., se propusieron los siguientes objetivos:

- Integración con dispositivos de seguridad física. La seguridad física es uno de los once dominios de la norma ISO 17799:2005, y tener la posibilidad de gestionar los dispositivos de seguridad física de la organización desde un punto central es, sin duda, una gran ventaja.
- Producción automática de directivas de correlación, con los fines de adecuar el comportamiento de OSSIM a las características del sistema informático de la organización, y facilitar la labor del administrador.
- Adicionalmente, se condujo un estudio con el objetivo de mejorar la confiabilidad de la captura de información en los sensores de red, en circunstancias de alto tráfico.

A continuación se exponen los resultados logrados en estas tres labores.

Integración con un panel de alarma de incendio

La mayoría de los paneles de alarma de incendio existentes en el mercado tienen la posibilidad de conectarse a una central de monitoreo remoto, empleando una línea telefónica. Una vez conectado, el panel transmite los datos de la alerta a la central, empleando una secuencia de tonos DTMF. El protocolo más usado para este propósito fue desarrollado por Ademco (hoy parte de Honeywell) y se le conoce como protocolo Contact ID (SIA, 1999).

La solución concebida para integrar un panel de alarma al sistema OSSIM se ilustra a continuación.

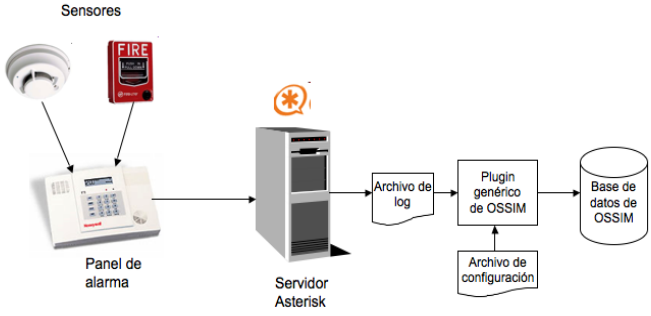

Figura 2. Integración de un panel de alarma de incendio con el sistema OSSIM

La salida telefónica del panel de alarma se conectó a un servidor Linux, dotado con una tarjeta Digium FXO/FXS para manejo de voz sobre IP, y el software Asterisk, que implementa un PBX IP (Asterisk, 2008). Seguidamente, se configuró bajo Asterisk el puerto FXS de la tarjeta con un número de extensión, y se configuró el panel de alarma para que marque dicho número de extensión en el momento en que requiera reportar algún evento.

La extensión se configura en Asterisk para que conteste automáticamente después de un cierto número de timbres, y para que ejecute la función AlarmReceiver() una vez conteste. AlarmReceiver() (2008) es una rutina incluida con la distribución de Asterisk, que se encarga de recibir la secuencia de

tonos DTMF enviada por el panel de alarma, decodificarla, y escribir el registro de la alarma en un archivo de log.

Se procedió entonces a diseñar un archivo para configuración del plugin genérico de OSSIM. El plugin convierte cada registro del archivo de log al formato estándar empleado por OSSIM, y registra la información en la base de datos. Además, traduce los códigos numéricos de la alarma a cadenas de texto fácilmente interpretables por un operador humano.

Esta solución tiene la ventaja que, con mínimos cambios al archivo de configuración del plugin, puede emplearse con cualquier alarma (ambiental, contra ladrones, de incendio, etc.) que emplee el protocolo Contact ID.

Integración de OSSIM con cámaras IP de vigilancia

De acuerdo con la norma ISO 17799:2005, debe existir un perímetro de seguridad física en toda instalación que contenga equipos de procesamiento de datos, y deben existir sistemas que detecten la presencia de intrusos dentro de dicho perímetro. Los sistemas de circuito cerrado de televisión (CCTV) han sido empleados por muchos años para este propósito en áreas que así lo requieren, tales como bancos, almacenes, centros comerciales y viviendas, entre otros.

Una de las grandes desventajas de estos sistemas en el pasado era la necesidad de supervisión continua de los monitores conectados a las cámaras, con el fin de poder detectar a tiempo un acceso no autorizado a determinada área. En caso de no haber nadie presente supervisando los monitores, era posible revisar posteriormente la grabación para encontrar evidencia del acceso no autorizado.

En la actualidad, los sistemas de grabación digital (Digital Video Recorders, DVR) permiten, además de almacenar el video capturado por las cámaras, procesarlo mediante algoritmos de detección de movimiento (Axis, 2008). Se pueden entonces demarcar zonas dentro del campo de visión de las cámaras, de tal manera que si el algoritmo de detección de movimiento observa cambios en alguna de dichas zonas, notifique del evento al operador. El sistema de grabación procede también a marcar la sección del video en la que se detectó el movimiento para facilitar su posterior consulta.

ZoneMinder (2008) es una solución de código abierto, que permite implementar un sistema de monitoreo de cámaras de vigilancia con funciones de DVR, bajo el sistema operativo Linux. Se decidió emplear este software debido a la gran variedad de cámaras que soporta (cámaras USB, IP y de video estándar conectadas a través de una tarjeta de captura).

La siguiente figura ilustra la integración de ZoneMinder con el sistema OSSIM.

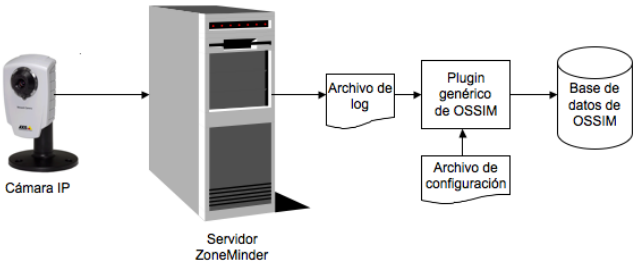

Figura 3. Integración de ZoneMinder con el sistema OSSIM

Como fuente de video se empleó una cámara IP. Se configuró a ZoneMinder sobre esta cámara, de tal manera que se generase un registro en el archivo de log cada vez que ocurriese movimiento en alguna de las zonas definidas en el cuadro de imagen. Igual que en el caso anterior, se escribió un archivo de configuración para el plugin genérico de OSSIM, quien se encarga de registrar el evento en la base de datos de OSSIM. A futuro, se desea modificar la consola forense de OSSIM, de tal manera que al seleccionar el evento generado por ZoneMinder, se abra la consola de ZoneMinder y se pueda ver el segmento de video que causó la alerta.

Mejora de la confiabilidad de la captura de paquetes en redes de alto tráfico

Algunos de los sensores más importantes de OSSIM, tales como Ntop (2008) y Snort (2008), emplean captura de paquetes para recolectar estadísticas y detectar anomalías en la red. El núcleo de Linux no viene afinado en su configuración por omisión para

soportar captura de paquetes en redes de alto tráfico, debido a las siguientes razones (Benvenuti, 2006):

- En modalidad de procesamiento promiscuo (que es la empleada durante la captura de tráfico), el núcleo de Linux crea dos copias del paquete. Una de ellas se dirige al socket abierto por la aplicación de captura, la otra continúa su procesamiento normal en la pila de protocolos del sistema operativo. En la mayoría de los casos esta última copia se descarta, ya que el paquete no va dirigido en la mayoría de los casos al equipo en el que se efectúa la captura. Puede ocurrir entonces pérdida de paquetes, o bien por el gran uso de tiempo de procesamiento que suponen todas estas operaciones, o bien por desbordamiento de buffers de paquetes en el núcleo.
- La mayoría de los controladores (drivers) de tarjetas de red en Linux operan en modalidad de interrupciones; es decir, cada vez que se recibe un paquete, la tarjeta de red interrumpe al procesador para que el sistema operativo reciba el paquete. En circunstancias de tráfico muy alto, el procesador podría pasar más tiempo atendiendo interrupciones de la tarjeta de red, que ejecutando otras funciones igualmente importantes. Este uso desbalanceado de los recursos también puede llevar a pérdida de paquetes.

En pruebas realizadas por el equipo de trabajo se pudo comprobar que, durante la captura en una red Fast Ethernet (100 Mbps) al 90% de su capacidad, se llegó a perder el 55% de los paquetes con la configuración original del núcleo de Linux, según se puede ver en la figura 4.

Se implementaron entonces los siguientes afinamientos en el núcleo Linux de las máquinas dedicadas a captura:

- Habilitación de sockets tipo PF_RING (Pfring, 2008) para la captura. Este tipo de socket minimiza el tiempo de tránsito de los paquetes por el kernel de Linux, mediante el uso de memoria compartida y de un buffer de anillo.
- Habilitación de la NAPI (New Network API) (Benvenuti, 2006) en el núcleo de Linux. NAPI permite que el kernel de Linux maneje los paquetes entrantes con un esquema híbrido entre interrupciones y polling, que comparado con el esquema de sólo interrupciones, procesa más rápidamente la llegada de múltiples paquetes a una misma interfaz, con menor consumo de procesador.

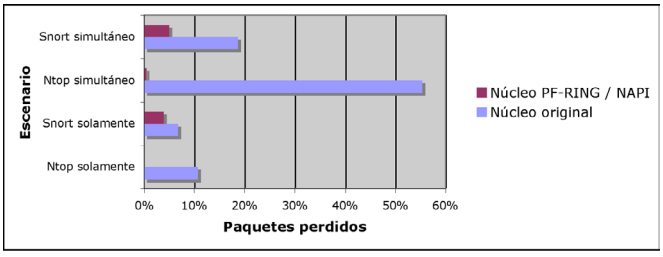

Figura 4. Comparación de pérdida de paquetes en el protocolo ICMP

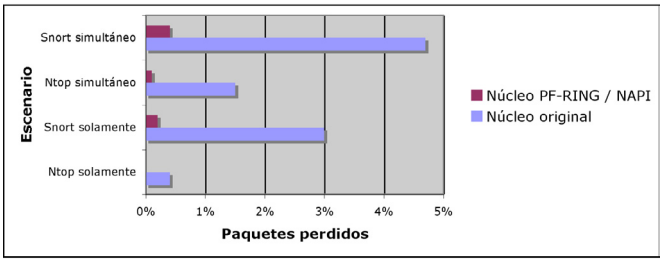

Figura 5. Comparación de pérdida de paquetes en el protocolo UDP

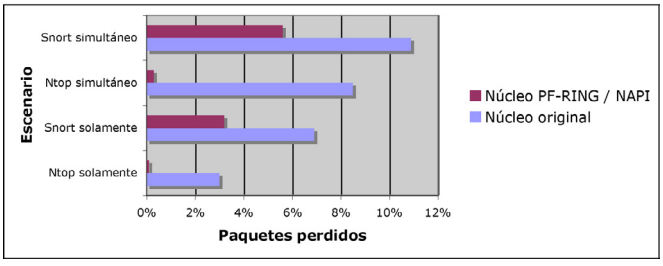

Figura 6. Comparación de pérdida de paquetes en el protocolo TCP

En los experimentos realizados por el grupo se encontró que este afinamiento disminuyó sustancialmente las estadísticas de pérdida de paquetes (véanse las figuras 4, 5 y 6), llegando a ser dicha pérdida del 5.6% a lo sumo, en condiciones de carga de la red similares a las del experimento con núcleo Linux sin modificar.

Producción automática de directivas de correlación

El motor de correlación de OSSIM efectúa tres tipos de correlación sobre los eventos que se registran en la base de datos (Casal, 2008):

- Correlación lógica: Trabaja con base en una serie de reglas llamadas directivas de correlación, que especifican las condiciones que se deben cumplir para que un evento o una serie de eventos registrados en la base de datos puedan generar una alarma.
- Correlación por inventario: Determina si un ataque en particular puede tener éxito en una determinada plataforma. Se emplea para descartar falsos positivos.
- Correlación cruzada: Valida la información detectada por un sensor con los datos obtenidos por otros sensores de la red. Permite descartar falsos positivos o elevar la categoría de una alarma.

El equipo de trabajo decidió implementar un módulo de software que corriera independientemente del motor de correlación, ya que la complejidad de dicho motor es bastante alta y el tiempo de desarrollo hubiera sobrepasado los límites impuestos por el proyecto. El módulo implementado consiste en un sistema de generación automática de directivas de correlación. Se tomó esta decisión porque OSSIM viene por omisión con un conjunto limitado de directivas, siendo labor del administrador del sistema afinar dicho conjunto de reglas de acuerdo con las características del sistema en particular, proceso que es largo y engorroso. Un generador automático de directivas es, por lo tanto, una gran ayuda para el administrador.

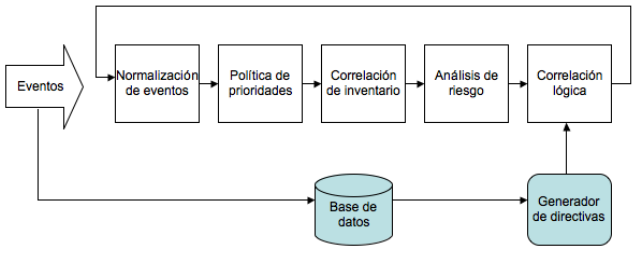

Figura 7. El generador automático de directivas en la arquitectura de OSSIM

Las directivas se generan a través de un algoritmo de clustering (Julish, 2003) que se corre sobre la base de datos de eventos. De este modo, dichas directivas se adaptan en alto grado a las condiciones particulares de la red bajo análisis.

Los eventos de la base de datos se agrupan de acuerdo con las direcciones fuente y destino de los mismos, así como por el puerto reportado en el evento. Las direcciones se agrupan de acuerdo con su procedencia (externas, en zona desmilitarizada o internas). Dicho esquema de agrupamiento se puede observar en la figura 8. Una vez que un grupo de eventos sobrepasa cierto tamaño, se genera automáticamente una regla nueva, que recoge las características comunes de los eventos agrupados.

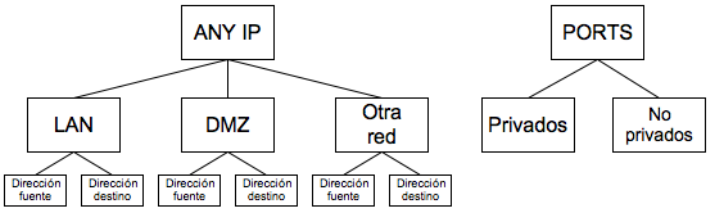

Figura 8. Jerarquías para agrupación de eventos

Las reglas así creadas son validadas entonces por un experto humano, antes de implementarlas en el ambiente de producción.

Conclusiones

La consola OSSIM presta un invaluable servicio al administrador de un sistema informático, brindándole información útil para la toma de decisiones en el campo de la seguridad informática. Con la intención de mejorar una herramienta de muy buena calidad, el equipo investigador logró desarrollar las interfaces necesarias para integrar un panel de alarma de incendios y un sistema de cámaras de vigilancia IP a la consola OSSIM, mejorar la confiabilidad de sus sistemas de captura de tráfico, y crear un módulo de generación automática de directivas de correlación.

La solución implementada emplea en su totalidad software libre de código abierto, por lo cual preserva la filosofía original de OSSIM, y permite su implementación a un costo relativamente bajo.

Este desarrollo ha permitido a la empresa Sistemas TGR, S.A., de la ciudad de Cali (Colombia), ofrecer a las empresas de la región los servicios de montaje

y configuración de consolas de seguridad informática, y el monitoreo centralizado de las mismas, mediante la implementación de un centro de gestión de seguridad informática (SOC Colombia).

Este trabajo muestra el enorme potencial que existe en Colombia para el desarrollo de servicios de consultoría en tecnologías de información y comunicaciones empleando herramientas de código abierto, y se convierte en un excelente ejemplo de colaboración entre universidad y empresa privada en este entorno.

Reconocimientos

Este trabajo de investigación fue financiado en parte por Colciencias y la Gobernación del Valle del Cauca, en el marco de la convocatoria 041/2007: «Concurso público de méritos para la financiación de proyectos basados en investigación, desarrollo tecnológico e innovación en el marco del fortalecimiento de la competitividad de las apuestas productivas estratégicas del Departamento del Valle del Cauca». Como entidad ejecutora del proyecto participó la Universidad Icesi, y como entidad beneficiaria, Sistemas TGR, S.A.

Referencias

AlarmReceiver (2008). Asterisk Alarmreceiver - SIA (Ademco) Contact ID Alarm Receiver Application. Consultado el 5 de Septiembre de 2008 en: http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+AlarmReceiver

Asterisk (2008). The Open Source PBX & Telephony Platform. Consultado el 5 de Septiembre de 2008 en: http://www.asterisk.org

Axis (2008). Axis Communications. Video Motion Detection (VMD). Consultado el 5 de septiembre de 2008 en: http://www.axis.com/products/video/about_networkvideo/vmd.htm

Benvenuti, Christian (2006). Understanding Linux Network Internals. O'Reilly, USA. Chapter 10: Frame Reception, pp. 210-238.

Carracedo, G. Justo (2004). Seguridad en redes Telemáticas. McGraw-Hill, España. Capítulo 1, pp 1-32.

Casal, Julio (2008). OSSIM: General Description Guide. Consultado el 5 de Septiembre de 2008 en: http://www.ossim.net/dokuwiki/doku.php?id=documentation:general_description

Congreso Estados Unidos (2002). United Status Congress. Sarbanes-Oxley Act of 2002. Consultado el 5 de Septiembre de 2008 en: http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf

ISO 17799 (2005). International Standards Organization (ISO). Information technology - Security techniques - Code of practice for information security management (Norma ISO/IEC 17799:2005), pp 115.

ISO 27001 (2005). International Standards Organization (ISO). Information technology - Security techniques - Information security management systems - Requirements (Norma ISO/IEC 27001:2005), pp 34.

Julish, Klaus (2003). Clustering Intrusion Detection Alarms to Support Root Cause Análisis. ACM Transactions on Information and System Security, Vol. 6, No. 4, November, pp 443-471.

Ntop (2008). Consultado el 5 de Septiembre de 2008 en: http://www.ntop.org

OSSIM (2008). Open System Security Information Management. Consultado el 5 de Septiembre de 2008 en: http://www.ossim.net

Ossim Agent (2008). OSSIM: Agent Documentation. Consultado el 5 de septiembre de 2008 en: http://www.ossim.net/dokuwiki/doku.php?id=documentation:agent#plugins

Pfring (2008). PF-RING overview. Consultado el 4 de octubre de 2008 en: http://www.ntop.org/PF_RING.html

SIA (1999). Security Industry Association. Digital Communication Standard - Ademco (r) Contact ID Protocol - for Alarm System Communications. Consultado el 5 de Septiembre de 2008 en: http://www.smartelectron.ru/files/DC-05_Contact_ID.pdf

Snort (2008). The de facto standard for intrusion detection / prevention. Consultado el 5 de Septiembre de 2008 en: http://www.snort.org

Unión Europea (2000). Protección de datos en la Unión Europea. Consultado el 5 de Septiembre de 2008 en: http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-spain_es.pdf

ZoneMinder (2008). Linux Home CCTV and Video Camera Security with Motion. Consultado el 5 de Septiembre de 2008 en: http://www.zoneminder.com/

Sobre los autores

Juan Manuel Madrid Molina
Ingeniero de Sistemas y Especialista en Gerencia de Informática de la Universidad Icesi. Cursó estudios doctorales en Ciencias de la Computación en la Universidad de Kansas. Es profesor investigador de tiempo completo y director del programa de Ingeniería Telemática de la Universidad ICESI. Sus áreas de interés son la seguridad informática, y la planeación y gestión de sistemas informáticos.

Luis Eduardo Múnera Salazar
Matemático de la Universidad del Valle, Magíster y Doctor en Informática de la Universidad Politécnica de Madrid. Se desempeña como profesor investigador de tiempo completo en la Universidad Icesi. Sus campos de investigación son la inteligencia artificial y las bases de datos.

Carlos Andrey Montoya González
Ingeniero de Sistemas, Especialista en Gerencia de Informática Organizacional y Especialista en Redes y Comunicaciones de la Universidad ICESI. Se desempeña como administrador de redes, profesor e investigador en la Universidad ICESI.

Juan David Osorio Betancur
Ingeniero Telemático de la Universidad ICESI, profesor e investigador de la misma Universidad, vinculado al grupo i2T. Ha realizado investigación en el área de desarrollo de aplicaciones móviles, planeación de redes inalámbricas y computación en malla aplicada a problemas de finanzas y economía.

Luis Ernesto Cárdenas
Ingeniero Electrónico de la Universidad del Valle. Tiene experiencia en técnicas de inteligencia computacional, procesamiento digital de señales y de imágenes, desarrollo de aplicaciones visuales, programación de microcontroladores, interfaces e instrumentación. Actualmente se desempeña como gerente general de Genia Tecnología, profesor hora cátedra de la Universidad ICESI e investigador vinculado al grupo i2T de la misma Universidad.

Rodrigo Bedoya
Ha cursado estudios en Ingeniería Eléctrica y Electrónica en la Universidad Autónoma. Tiene amplia experiencia en administración y monitorización de seguridad en redes, montajes e implementaciones de defensa en profundidad, y experiencia en hacking ético. Trabaja actualmente en Sistemas TGR, S.A.

Cristian Latorre
Estudiante de Física de la Universidad del Valle, y desarrollador de software en Sistemas TGR S.A. Sus áreas de interés son: Instrumentación Electrónica, Seguridad Informática, Plataformas UNIX / POSIX.