



EVENCO CCC

IMPLEMENTACIÓN Y MEJORA DE LA CONSOLA DE SEGURIDAD INFORMÁTICA OSSIM EN EL ENTORNO COLOMBIANO

JUAN MANUEL MADRID MOLINA, CARLOS ANDREY MONTOYA GONZÁLEZ, JUAN DAVID OSORIO BETANCUR, ANDRÉS VÁSQUEZ, LUIS EDUARDO CÁRDENAS, LUIS EDUARDO MÚNERA SALAZAR, RODRIGO BEDDOYA, CRISTIAN LATORRE.

Resumen— Una de las herramientas más usadas hoy en día para la gestión de la seguridad informática en las empresas es la consola de seguridad. Este artículo resume el trabajo efectuado por nuestro equipo de investigación para integrar una serie de mejoras a la consola de seguridad informática OSSIM para adaptarla al entorno colombiano. Dichas mejoras incluyen la interconexión con dispositivos de seguridad física, la 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.

I. INTRODUCCIÓN

La gestión de la seguridad informática se ha convertido en una necesidad para las organizaciones de hoy, debido a exigencias legales [1, 2] y de cumplimiento con estándares internacionales [3, 4].

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, que se pueden emplear para verificar el cumplimiento de indicadores de gestión.

Una de las consolas de gestión de código abierto más populares en la actualidad es OSSIM [5]. Esta consola, además de recolectar y uniformizar los eventos de los diferentes sistemas, correlaciona los eventos que ocurren en el sistema bajo análisis, con el fin de minimizar el número de alertas que el administrador recibe y eliminar falsos positivos.

Este artículo describe el trabajo realizado por nuestro 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.

II. PROBLEMÁTICA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Para que un sistema informático se considere como seguro, debe cumplir con cuatro premisas básicas [6]:

- 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*, o sea 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.
- 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, debido al descubrimiento de nuevos métodos de ataque.

Por otro lado, la legislación de los diferentes países se ha ido actualizando con el fin de castigar el delito informático, pero a la vez exige que se disponga de un nivel adecuado de protección en los sistemas de información [1, 2]. La seguridad de la información también se ha convertido en asunto crítico para procesos de calidad total de las empresas y estrategias

TELÉFONO: (5) 3730507

WWW.EVENCOCCC.COM

EVENCOCCC@EVENCOCCC.COM

BARRANQUILLA -- COLOMBIA



EVENCO CCC

de gobierno de tecnologías de información. En todos estos procesos no solamente se exige que existan mecanismos que garanticen la seguridad [3], sino que se requiere cuantificar su impacto mediante el uso de indicadores [4].

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 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, 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 periodo 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 este, 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.

III. GENERALIDADES Y ARQUITECTURA DE OSSIM

La plataforma OSSIM (Open System Security Information Management) [5] 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 programas y dispositivos de seguridad. La arquitectura de OSSIM es distribuida y comprende cuatro elementos básicos [7]:

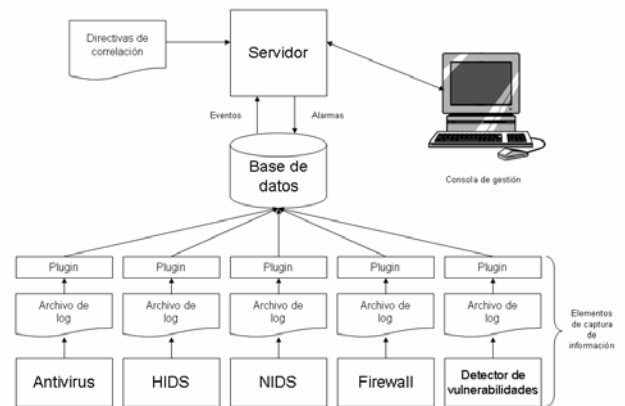


Figura 1. Arquitectura de OSSIM

- **Elementos de captura de información:** Recolectan la información requerida por OSSIM, en los diferentes sitios del sistema informático en donde se desea hacer control.
- **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



EVENCO CCC

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.

IV. 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:

- Montaje y documentación total del sistema.
- Integración con dispositivos de seguridad física
- Producción automática de directivas de correlación

A continuación se explica la manera cómo se lograron estos objetivos. La mejora de la confiabilidad en la captura de información en redes de alto tráfico fue un resultado adicional no considerado en los objetivos iniciales, pero que igual se describe por la importancia que reviste.

A. 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 se conoce como Contact ID [8].

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

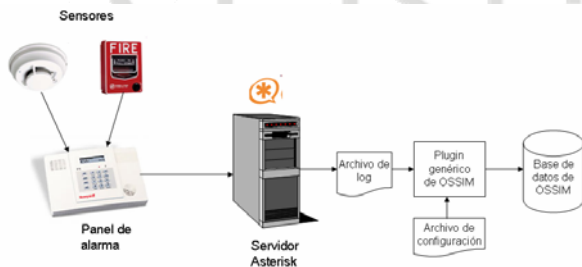


Figura 2. Integración de un panel de alarma de incendio con el sistema OSSIM

La salida telefónica del panel de alarma se conectó a un servidor Linux, dotado con una tarjeta FXO/FXS para manejo de voz sobre IP, y el software Asterisk, que implementa un PBX IP [9]. 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 marcara 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() [10] 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.

B. 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, viviendas, etc.

ZoneMinder [11] es una solución de código abierto, que permite implementar un sistema de monitoreo de cámaras de vigilancia con funciones de detección de movimiento bajo el sistema operativo Linux. Se decidió emplear este software debido a la gran variedad de cámaras que soporta.

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

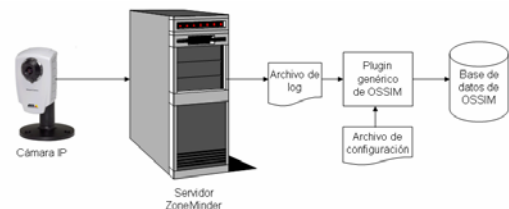


Figura 3. Integración de ZoneMinder con el sistema OSSIM



EVENCO CCC

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.

C. 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 [12] y Snort [13], 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; esto puede ocasionar la pérdida de hasta el 55% de los paquetes en una red Ethernet de 100 Mbps operada al 90% de su capacidad. Se implementaron entonces los siguientes afinamientos en el kernel Linux de las máquinas dedicadas a captura:

- **Habilitación de sockets tipo PF_RING [14] 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) [15] en el kernel 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 (habilitado en Linux por omisión), procesa más rápidamente la llegada de múltiples paquetes a una misma interfaz, con menor consumo de procesador.

En los experimentos realizados por nosotros, se encontró que este afinamiento disminuyó sustancialmente las estadísticas de pérdida de paquetes, llegando a ser dicha pérdida del 5.6% a lo sumo, en condiciones de carga de la red similares a las del experimento con kernel sin modificar.

D. 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 [7]:

- **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.

Nuestro equipo de trabajo decidió implementar un sistema de generación automática de directivas de correlación, debido a que OSSIM viene por omisión con un conjunto limitado de directivas. El administrador de la red debe afinar dicho conjunto de reglas de acuerdo con las características de dicha red, proceso que es largo y engorroso.

Las directivas se generan a través de un algoritmo de clustering [16] 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. Las reglas así creadas son validadas entonces por un experto humano, antes de implementarlas en el ambiente de producción.



EVENCO CCC

V. 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, nuestro 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, 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 nuestro 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

- [1] Unión Europea. Protección de datos en la Unión Europea. 2000. http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-spain_es.pdf .
- [2] United Status Congress. Sarbanes-Oxley Act of 2002. 23 de enero de 2002. <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf> .
- [3] International Standards Organization (ISO). Information technology – Security techniques – Code of practice for information security management (Norma ISO/IEC 17799:2005). Junio de 2005. 115 pp.
- [4] International Standards Organization (ISO). Information technology – Security techniques – Information security management systems – Requirements (Norma ISO/IEC 27001:2005). Noviembre de 2005. 34 pp.
- [5] OSSIM (Open System Security Information Management). <http://www.ossim.net>
- [6] Carracedo Gallardo, Justo. Seguridad en redes Telemáticas. McGraw-Hill, España, 2004. Capítulo 1, 1-32 pp.
- [7] Casal, Julio. OSSIM: General Description Guide. http://www.ossim.net/dokuwiki/doku.php?id=documentation:general_description .
- [8] Security Industry Association. Digital Communication Standard - Ademco ® Contact ID Protocol - for Alarm System Communications. http://www.smartelectron.ru/files/DC-05_Contact_ID.pdf .
- [9] Asterisk – The Open Source PBX & Telephony Platform. <http://www.asterisk.org>
- [10] Asterisk Alarmreceiver - SIA (Ademco) Contact ID Alarm Receiver Application. <http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+AlarmReceiver>
- [11] ZoneMinder: Linux Home CCTV and Video Camera Security with Motion. <http://www.zoneminder.com/>
- [12] Ntop. <http://www.ntop.org>
- [13] Snort – the de facto standard for intrusion detection / prevention. <http://www.snort.org>
- [14] PF-RING overview. http://www.ntop.org/PF_RING.html
- [15] Benvenuti, Christian. Understanding Linux Network Internals. O'Reilly, USA, 2006. Chapter 10: Frame Reception, 210-238 pp.
- [16] Julish, Klaus. Clustering Intrusion Detection Alarms to Support Root Cause Analysis. ACM Transactions on Information and System Security, Vol. 6, No. 4, November 2003. 443–471 pp.