Autoritat de Certificació
de la Comunitat Valenciana

Implantación de OSSIM en la Autoridad de Certificación de la Comunidad Valenciana

Angel Alonso Párrizas
aalonso@accv.es
CISSP, CCNA,
SANS SSP-MPA, SANS SSP-CNSA

Julio de 2.007

Agenda

- Objetivos del proyecto
- Como se conoció la plataforma
- Implantación de OSSIM en la ACCV
- Conclusiones
- Bibliografía

Objetivos del proyecto

- ✓ **Implantación de un sistema de detección de intrusos distribuido**
- ✓ **Homogeneización y centralización de la información de eventos.**
- ✓ **Monitorización desde una perspectiva de Integridad y confidencialidad.**
- ✓ **Sustitucion de la plataforma propietaria existente por una open source**
- ✓ **Monitorización de la red y los sistemas (C e I)**
- ✓ **Posibilidad de integrar con los productos propietarios existentes (FW1 y Fortigate)**

¿Cómo se conoció la plataforma OSSIM?

Proyecto de investigación con RedIRIS: ELAS

Técnicas de programación de Buffer Overflows y Heap Overflows

Valoración de distintas herramientas open-source existentes para detectar distintos ataques

Objetivo: correlar los datos de la red con los datos de los hosts.

Herramientas:

NIDS: Prelude (a su vez correla y centraliza la información). Bro (IDS a nivel de aplicación)

HIDS/HIPS: Systrace (parche para el kernel). Captura las llamadas al sistema, enjaula (chroot) aplicaciones, elimina la necesidad de ejecución mediante los bits de SETUID y SETGID.

¿Cómo se conoció la plataforma OSSIM?

Proyecto de investigación con RedIRIS: ELAS

Estandarización de formatos de alertas para intrusiones: IDMEF(XML)

Se conoce OSSIM como herramientas centralizadora y correladora:

- Tiene parses para Prelude
- Permite centralizar sistemas IDS distribuidos
- Más completa que Prelude
- Utiliza Snort como base.
- Permite monitorización a más niveles (no sólo nivel 4 y 7)

Se conoce OSSEC como herramienta centralizadora y correladora:

- Se centra solo en los hosts (HIDS, logs de auditoría..)

✓ **Finalmente se implementa una plataforma DIDS con OSSIM (snort, nessus, logs Apache, OSIRIS y reglas de correlación)**

- Se comprueba la correlación con datasets

Implantación de OSSIM en la ACCV

- **Se pretendía migrar el sistema propietario existente (Enterasys) por uno OpenSource**
  - ✓ Coste de licencias
  - ✓ Personal con conocimiento para su administración.
- **El impacto en los sistemas debía ser mínimo e igual para todos.**
  - ✓ Muchos HIDS necesitan parches para el kernel
  - ✓ Debía de integrase un HIDS en todas las plataformas (Solaris, Linux, Windows).
- **El NIDS debía cubrir todas las DMZs**
- **Se centró en la C e I. La A ya se monitorizaba con otras herramientas con asistencia 24 x 7.**

Implantación de OSSIM en la ACCV

- **¿Qué NIDS?**
  - ✓ **Snort:**
    - **Gran cantidad de firmas**
    - **Motor de anomalías (Spade)**
    - **Abundante documentación y foros.**
    - **Flexibilidad a la hora de configurar**
    - **Conocimiento de la herramienta**
    - **Snort_inline como NIPS (no está activo).**
    - **Acid Base está integrado en OSSIM**

Implantación de OSSIM en la ACCV

- **¿Qué HIDS?**
  - ✓**OSIRIS**
    - •Multiplataforma: Linux, Solaris, Windows, AIX, IRIX, BSD, Mac OS X.
    - •Gestión de manera centralizada.
    - •Comunicación entre cliente-servidor por SSL.
    - •Monitoriza la integridad de los ficheros, cambios en usuarios/grupos, cambios en puertos a la escucha, modulos en el kernel.
    - •Compilar y ejecutar (no necesita parches para el kernel).
    - •Para cada SO se crea un perfil en función de las necesidades

Implantación de OSSIM en la ACCV

- **Además se pretende monitorizar los eventos del SO.**
  - ✓ En Unix los logs de auditoría se redireccionan mediante un syslog
    - /var/log/auth.log
  - ✓ En windows se instala Snare
    - Monitoriza los accesos, cambios de políticas de seguridad, cambios de contraseñas, etc.

- **En este punto, se tienen definidas las herramientas a usar, que nos dan una visión 'a vista de pajaro y desde el interior' de la seguridad de los sistemas**
- **Pendiente: Integrar todas estas herramientas, centralizarlas, tener un portal para visionar los eventos, poder crear prioridades a los eventos, etc, etc**

Implantación de OSSIM en la ACCV

Ossim-server y Ossim-framework

- Un único sistema donde centralizar la información.
- Un único sistema donde analizar la información
- Un único sistema desde el que envíar información (alertas por mail)
- Simplicidad, sencillez, rápida gestión

- Además en este servidor corre el servidor de logs. A el llegan logs de todos los sistemas y de los FWs (se parsean muchos de los logs en este sistema).
- Este sistema alberga las BBDD.
- Este sistema es el manager de los HIDS.

Implantación de OSSIM en la ACCV

Ossim-agent

- Para cada DMZ se tiene un sistema con el agent instalado.
- Sistema totalmente distribuido y que permite tener visión de todas las redes.
- Sistemas con triple interfaz de red (conmutadores LAN estacados) para capturar tráfico del port-mirroring configurado en los switches.
- Snort en cada 'ossim-agent' con actualización de firmas diaria.
- Arpwatch para monitorizar cualquier problema a nivel 2.

- Importante: configuración del NIDS precisa y acorde a los servicios de cada DMZ (nos evitamos muchos falsos positivos y trabajo de CPU)

Implantación de OSSIM en la ACCV

Configuración del servidor (Ossim-server)

- Reglas específicas de correlación para eventos determinados.
- Ante ciertos eventos críticos se envía correo al administrador de seguridad.
- Algunos ejemplos:
  - Error en la autenticación del usuario.
  - Cambio en la política de windows
  - Modificación en el Sistema de ficheros
  - Alerta del NIDS.

Implantación de OSSIM en la ACCV

Informes de los eventos

•La plataforma permite crear informes de los eventos más relevantes, sistemas involucrados, etc

•Nos da flexibilidad para poder realizar los informes periódicos sobre cualquier problema en sistemas que albergan datos de carácter personal (LOPD)

•Se puede analizar la evolución.

•Aunque la parte más importante es la monitorización de los eventos correlados en tiempo real y el envío de correo.

Implantación de OSSIM en la ACCV

Conclusiones

- **Tenemos un sistema que cumple los requesitos planteados.**
- **Tenemos una visión de qué ocurre en nuestros sistemas desde todos los ángulos.**
- **Tenemos un único punto donde se centraliza la información.**
- **Todos las herramientas son 'open-source', lo que nos da flexibilidad.**
- **Es factible la integración de la información generada por cualquier dispostivo de seguridad (ACLs, FW1, NIPS..).**
- **Avisos en tiempo real de la violación de la política de seguridad.**

Bibliografía

- Prelude IDS: http://www.prelude-ids.org/
- Bro IDS: http://www.bro-ids.org/
- Systrace HIDS/HIPS: http://www.citi.umich.edu/u/provos/systrace/es/index.html
- IDEMF: http://xml.coverpages.org/IDMEF-provisional-draft-ietf-idwg-idmef-xml-02.html
- Snort Inline: http://snort-inline.sourceforge.net/
- OSSEC:
- OSIRIS HIDS: http://osiris.shmoo.com/
- OSSEC SIM: http://www.ossec.net/

Autoritat de Certificació
de la Comunitat Valenciana

GENERALITAT VALENCIANA

www.accv.es

Angel Alonso Párrizas
Tel. 961 961 176
Fax. 961 961 002
aalonso@accv.es