



# ***Propuesta de una arquitectura de sistemas de detección de intrusos con correlación.***

**Autor: Angel Alonso Párrizas  
Director: Santiago Felici Castell**



- **Introducción**
- **Objetivos**
- **Estado del Arte**
- **Red a Monitorizar**
- **IDSs utilizados**
- **OSSIM**
- **Reglas de correlación utilizadas.**
- **Resultados**
- **Conclusiones**
- **Trabajo futuro**



- Las redes de ordenadores pueden presentar **vulnerabilidades** que pueden ser aprovechadas por atacantes teniendo un impacto negativo sobre los activos. (DoS, escalada de privilegios, infecciones víricas..).
  
- Existen una gran variedad de **herramientas de seguridad** para minimizar el éste **riesgo**:
  - Firewalls, Routers, Proxys Inversos.. (seguridad perimetral)
  - Escaners de vulnerabilidades, herramientas de actualización, IPS.. (prevención)
  - Detectores de intrusos (IDS), antivirus ..(detección)
  - Monitores de eventos: logs de aplicaciones, logs del sistema operativo..



- Una red bien monitorizada puede disponer de mucha información de los eventos que ocurren: se cae en la “sobre información”.
- Los Sistemas de Detección de Intrusos (**IDS**) generan muchos “**falsos positivos**” y/o “**falsos negativos**”.
- Existen diferentes alternativas para resumir la información que es generada en una red:
  - Precisión.
  - **Correlación.**

Un ataque es capaz de generar muchas alertas pero el ataque es uno y único, por cada ataque real con intrusión fidedigna se ha de generar una única alarma.



- El objetivo principal es **correlar la información** de distintos sistemas de seguridad (detectores de intrusos, monitores de red, auditores de red, etc) con el fin de reducir el número de falsas alarmas.
  
- De forma más precisa se pretende:
  - Estudiar y evaluar las prestaciones de diferentes sensores .
  - Integrar diferentes sensores de libre distribución.
  - Implementar y utilizar diferentes reglas de correlación
  - Realizar una arquitectura general y abierta de correlación de alertas y contramedidas utilizando software de libre distribución.
  - Incluir distintas herramientas de seguridad: auditores de sistemas y analizadores de factor de riesgo.



- **Sistemas de detección de intrusos (IDS):** monitorizan los intentos de intrusión en un sistema informático (confidencialidad, integridad, disponibilidad y evasión de la seguridad).

Clasificación:

- Fuente de información: red (**NIDS**) y host (**HIDS**).
- Tipo de análisis: **abusos (firmas)** y anomalías.
- Tipo de respuesta: **Activa** (“Intrusion Prevention System”) y **pasiva**.

Herramientas de libre distribución:

- **Snort:** NIDS muy popular. Actualmente existen proyectos para desarrollo de firmas como “bleeding rules”.
- **Osiris:** HIDS que comprueba la integridad del Sistema de ficheros. Monitoriza también usuarios, grupos, y módulos del kernel. UNIX (incluyendo BSD), Linux, Mac OS X, AIX, IRIX y Windows NT/2000/XP.



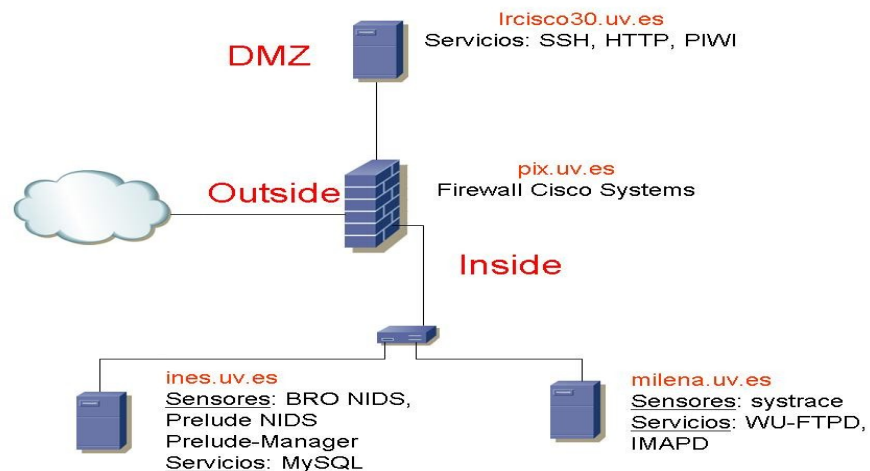
- **Systrace:** HIDS que captura las llamadas al sistema.
  - **Bro:** NIDS a nivel 4 y 7 basado en anomalías.
  - **Prelude:** Puede integrar diferentes sensores IDS.
- Formatos de alertas estándar: Intrusion Detection Message Exchange Format (**IDMEF**). Formato en XML.
- Nuevas Tendencias: Distributed Intrusion Detection System (DIDS).
- Se dispone de varios HIDS o NIDS que envían la información de los eventos a un controlador.
  - Redundancia, posible tolerancia a fallos, control sobre todos los segmentos de la red.



## ■ Otras herramientas:

- Análisis vulnerabilidades: **Nessus**.
- Servicios y versiones: **Nmap**.
- WebServices: Nikto.
- Herramientas de gestión y administración:
  - Ntop, Arpwatch, p0f y logs del sistema (Syslog, Apache..)

## ■ Proyecto ELAS.







### ■ Herramientas a utilizar:

- Nessus. Escaner de vulnerabilidades
- NIDS. Snort configurado con filtrado de reglas.
- HIDS, recolección de datos,
- Logs de aplicaciones (Apache).

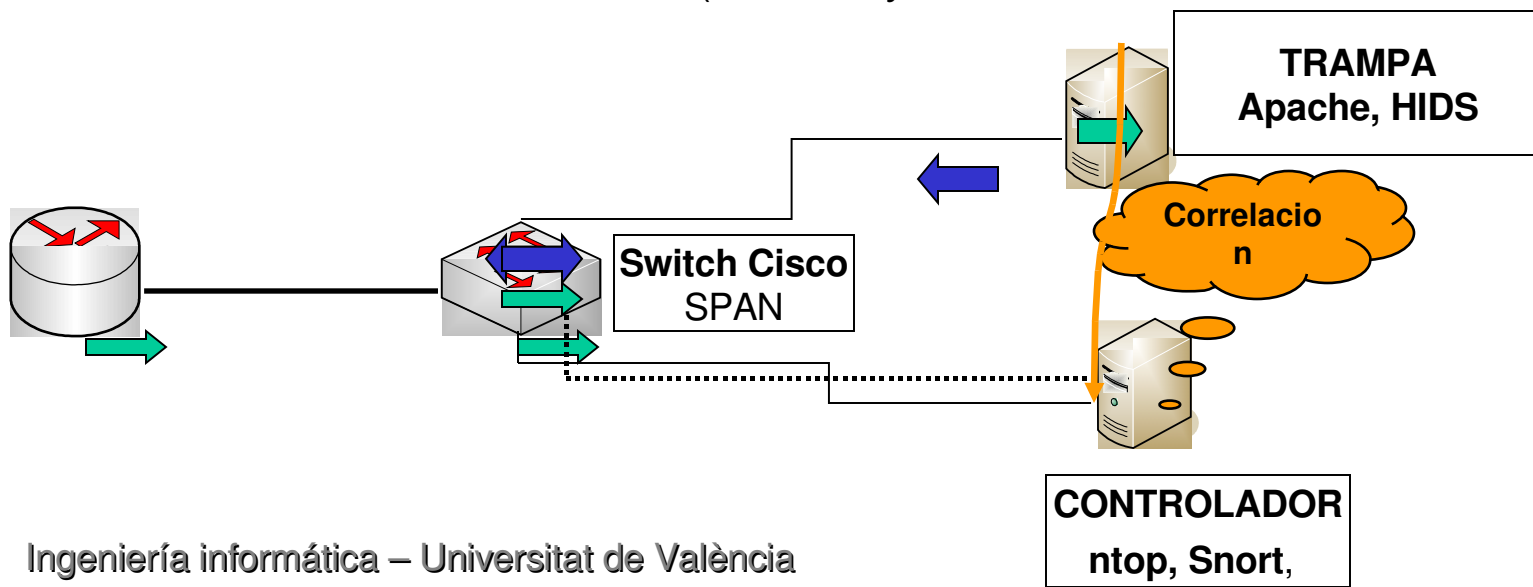
### ■ Correladores a utilizar:

- Mediante **algoritmos heurísticos**: acumulación en el tiempo y de eventos. Nivel de Compromiso (C) y nivel de ataque (A).
- Mediante **secuencia de eventos**.



- Modelo general de correlación (Giovanni Vigna. 1545-5971/04. IEEE July 2004).
  1. **Normalización:** todos los sensores generen las alertas en el mismo formato.
  2. **Preproceso:** completar los campos que vacíos.
  3. **Fusión de alertas:** alertas detectadas por distintos NIDS pero que se refieren a una misma alerta.
  4. **Verificación de alerta:** comprobar la veracidad de una alerta.
  5. **Reconstrucción del hilo de ataque:** alertas con misma IP origen y destino que se han lanzado en un mismo NIDS.
  6. **Reconstrucción de la sesión de ataque:** relación en el tiempo del NIDS y HIDS.
  7. **Reconocimiento foco del ataque:** “one2many”.
  8. **Correlación multipaso:** evolución del ataque.
  9. **Análisis del impacto.**
  10. **Priorización de alertas.**

- **Alerta**: evento monitorizado. **Alarma**: ataque real.  
La alarma es la consecuencia de varias alertas relacionadas.
- **SNORT**: captura el tráfico a nivel 2.
  - Se configura para que no genere alertas con tráfico multicast y ataques al servidor ISS.
- **APACHE**: Peticiones GET y POST con respuesta 400 ó 200.
- **NTOP**: conexiones TCP abiertas, consumos excesivos de ancho de banda, paquetes enviados.
- **OSIRIS**: sistema de ficheros: (<Directory /var/www/ > IncludeAll </Directory>)





## Open Source Security Information Management.

- Gestor de la seguridad de la información a nivel de riesgos y ataques.
- **Integrador** de diversas herramientas de seguridad (IDSs, Firewalls, routers, logs de aplicaciones..)
- **Correlador** mediante secuencias de eventos y algoritmos heurísticos.
- Análisis forense.
- Automatiza análisis de vulnerabilidades y detección de nuevos servicios en la red.
- Detector a nivel 2, nivel 3, nivel 4 y nivel 7.



- Detección: patrones y anomalías. Las anomalías se toman como información complementaria.
- Centralización / normalización: información de sensores y monitores.
- Priorización de las alertas.
- Valoración del riesgo.
- Consola forense y cuadro de mandos.
- Los elementos de OSSIM son tres:
  - **Ossim-agent** (agente monitor)
  - **Ossim-server** (Servidor y recolector de eventos)
  - **Ossim-framework** (interfaz para la gestión y configuración).
- Apache, Arpwatch, Cisco IDS, Firewall PIX de Cisco, Routers Cisco Firewall one de CheckPoint, Iptables, Internet Information Server, Ntop, Ntsyslog, Osiris, Prelude HIDS, Snort, Syslog, p0f, tcptrack, snarewindows, realsecure, rrd, opennms, netgear, Nagios



- (1) Debe detectar los eventos en la red. (Snort)
- (2) Debe de centrarse en la aplicación. (Apache)
- (3) Revisa los eventos a nivel de host (Osiris).
- (4) Detecta una conexión desde la máquina destino a cualquier otro host.

(1) `<directive id="4" name="correlacion NIDS APACHE HIDS CONEXION - VICTIMA" priority="5">`

`<rule type="detector" name="nids" reliability="1" occurrence="1" from="ANY" to="ANY" port_from="ANY port_to="ANY" plugin_id="1001" plugin_sid="ANY" >`

(2) `<rules> <rule type="detector" name="LOGS APACHE" reliability="3" occurrence="1" from="1:SRC_IP" to="1:DST_IP" port_from="ANY" port_to="ANY" plugin_id="1501" plugin_sid="ANY">`

`</rules>`



(3) `<rule type="detector" name="ALERTA OSIRIS" reliability="5" occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY" plugin_id="4001" plugin_sid="ANY">`

`</rules>`

(4) `<rule type="monitor" name="ALERTA CONEXION RARA" reliability="10" from="1:DST_IP" to="ANY" port_from="ANY" port_to="ANY" plugin_id="2005" plugin_sid="ANY"/>`

`</rules>`



- Las máquinas TRAMPA son: [glup.uv.es](http://glup.uv.es) y [labd.uv.es](http://labd.uv.es)
- Alertas de **Snort** en [glup.uv.es](http://glup.uv.es): (Con depurado de las reglas)
  - (portscan) Open Port 30%
  - (portscan) TCP Portscan 25%
  - (http inspect) IIS UNICODE CODEPOINT ENCODING 23%
  - (http inspect) BARE BYTE UNICODE ENCODING 22%
  - (http inspect) DOUBLE DECODING ATTACK 10%
- Análisis Vulnerabilidades (**Nessus**):
  - Máquina [glup.uv.es](http://glup.uv.es): 18% medium, 82% low.  
 **Securizada y bastionada.**
  - Máquina [labd.uv.es](http://labd.uv.es): 5% high (phf), 5% medium, 90% low.  
 -cgi phf y portal php-nuke vulnerable.



## Correlación:

Alertas totales: aproximadamente **10.000** (obtenida como la suma de las alertas del NIDS + logs de Apache).

Alarmas (ataques consumados): **50**

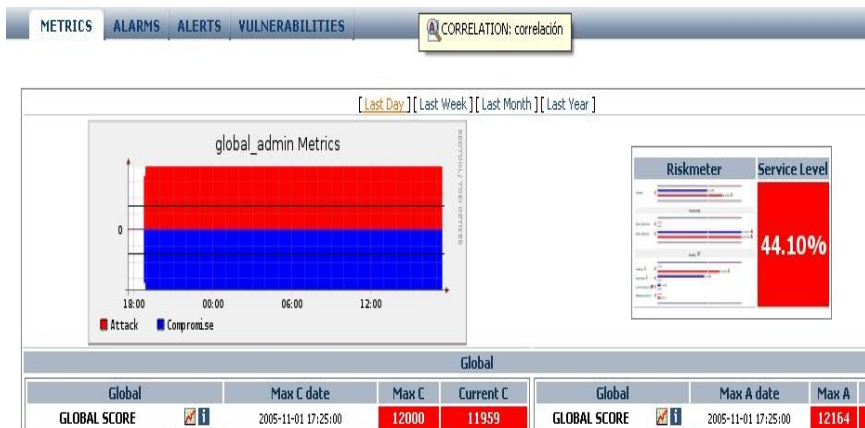
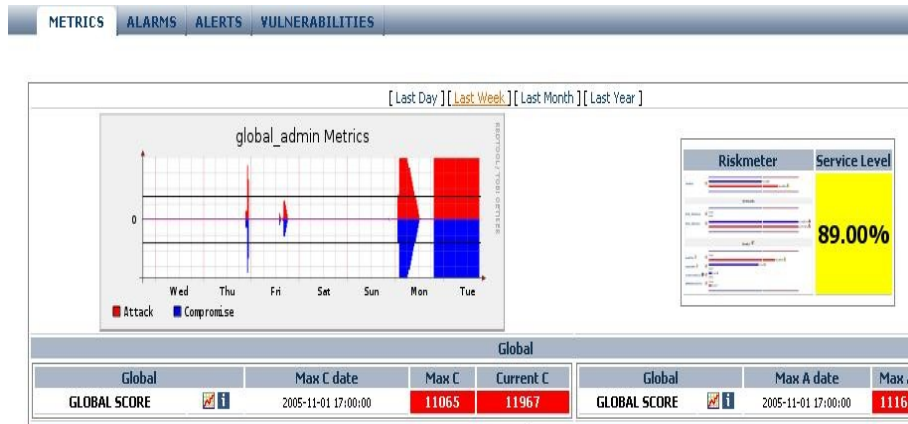
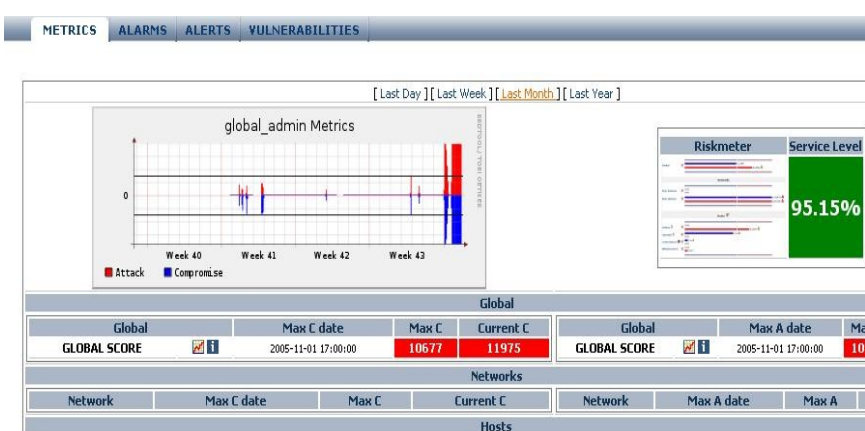
50/10.000  **200 a 1**

11	correlacion APACHE-NIDS-HIDS CONEXION VICTIMA A ATACANTE	10	147.156.222.109 127.0.0.1 labd	2005-1
12	correlacion APACHE-HIDS	10		
13	correlacion APACHE-NIDS-HIDS-CONEXION-DESDE_VICTIMA	10	labd 147.156.222.109 127.0.0.1	2005-1
14	correlacion APACHE-NIDS-HIDS CONEXION VICTIMA A ATACANTE	10	labd 147.156.222.109 127.0.0.1	2005-1
15	correlacion APACHE-HIDS	10		
16	correlacion NIDS HIDS	10		
17	correlacion APACHE-HIDS	10		
18	correlacion APACHE-HIDS	10		
19	correlacion NIDS HIDS	10		
20	correlacion APACHE-NIDS-HIDS	3		
21	correlacion APACHE-NIDS	8		
22	correlacion APACHE-NIDS	8		
23	correlacion APACHE-NIDS-HIDS	3		
24	correlacion APACHE-NIDS-HIDS	3		
25	correlacion APACHE-NIDS-HIDS	3		
26	correlacion APACHE-NIDS-HIDS	3		
27	correlacion APACHE-NIDS-HIDS	3		

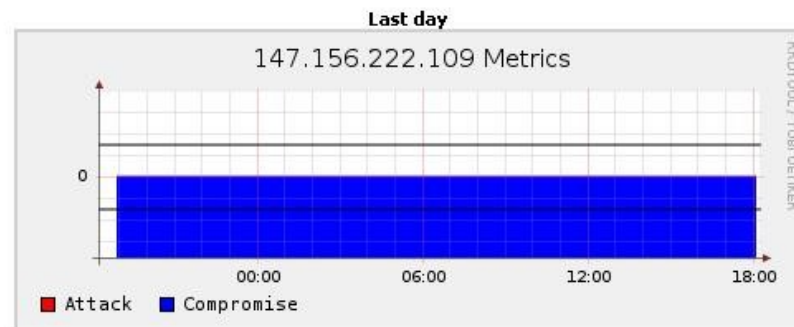




## Nivel de Ataque (A) y Compromiso (C)



Max C Level (last day)	10815	2005-11-01 13:20:00
Max C Level (last month)	10676	2005-11-01 15:00:00
Max C Level (last year)	10761	2005-11-01 13:30:00





- Se ha diseñado un sistema de detección de intrusos con correlación de eventos.
- Evaluación de diferentes herramientas código libre, integrándolas entre sí, obteniendo una buena cohesión entre ellas.
- Funcionamiento e integración de OSSIM tanto en la parte servidora como en los agentes, así como la integración con más herramientas de seguridad.
- Desarrollo de un modelo de correlación genérico, que relaciona los eventos en la red, con lo que sucede a nivel de aplicación y el impacto real sobre el host, mediante un HIDS.
- Reducción de las alertas en una tasa de 1:200



- Integración y pruebas con otras herramientas de seguridad.
- Pruebas en un entorno más hostil con sistemas heterogéneos, más tráfico, con el fin de valorar capacidades y rendimiento.
- Mejorar los traductores en Python e implementar más traductores para otras herramientas.
- Adaptar el modelo y la herramientas a otras herramientas de seguridad que no integre OSSIM.
- Crear directivas nuevas para ataques concretos.
- Estudiar la herramientas OSSIM como detector de anomalías.
- Integración de cifrado de manera nativa en las comunicaciones.
- Configurar la herramientas para que trabajen con IPS en lugar de IDS.
  
- En cuanto a la correlación
  - Sistemas de correlación para aplicaciones web basadas en anomalías.
  - Correlación de anomalías.



# ***Propuesta de una arquitectura de sistemas de detección de intrusos con correlación.***

**Autor: Angel Alonso Párrizas**  
**Director: Santiago Felici Castell**