Arquitectura de sensores de seguridad para la correlación de eventos

Lic. Javier Diaz
Lic. Nicolás Macia
Lic. Paula Venosa
Lic. Miguel Luengo
Ms. Lía Molinari
C.C. Viviana Ambrosi (*)

{ javierd, nmacia, pvenosa, mluengo, lmolinari, vambrosi } @ info.unlp.edu.ar
Calle 50 y 115 – 1er Piso – Edificio Bosque Oeste
L.I.N.T.I. - Facultad de Informatica – U.N.L.P.
(*) Profesional Principal - CICBA

Palabras Claves

Sistemas de detección de intrusiones, firewall, honeypot, correlación, NTP.

Resumen

El crecimiento exponencial que tuvo Internet en la última década trajo consigo un gran volumen de tráfico hostil. Es por ésto que implementar mecanismos de seguridad es una tarea imprescindible del administrador de red actual. Además el monitoreo de la seguridad de una red y sus sistemas es una pieza fundamental en la segurización de la misma puesto que permite una detección temprana de los incidentes de seguridad, para así responder en tiempo y forma y consecuentemente elaborar contramedidas a futuro.

Algunas aproximaciones más complejas consideran la sincronización de eventos de seguridad con una posterior correlación de tales eventos, con el objeto de obtener alertas más confiables. Una iniciativa de tal proyecto es el llevado a cabo por el ARCERT, llamada CAL "Coordinación y Análisis de Logs", el cual prevee la sincronización de eventos de seguridad dentro de las redes de los Organismos de la Administración Pública Nacional. Otra iniciativa similar es la de la UNAM, mediante el proyecto llamado Honeynet UNAM, el cual se basa en el uso de honeynets dentro del campus de la Universidad para el análisis de eventos de seguridad y la implementación de mecanismos pro-activos.

En este trabajo se presenta una arquitectura de sensores de seguridad distribuidos estratégicamente, de

modo de proveer la información recolectada a un monitor central en el que se lleven a cabo correlaciones de datos que permitan generar alertas confiables.

Introducción

Hoy en día es común detectar intentos hostiles para comprometer la seguridad de los sistemas. No resulta extraño que esos intentos provengan tanto desde el exterior como del interior de una organización.

Por ello, la necesidad de implementar mecanismos de seguridad como así también de monitorear el nivel de compromiso de las redes, es una tarea obligada que determinó la aparición de gran cantidad de herramientas que pueden ser usadas de diferentes maneras para atacar este problema. Entre estas herramientas se pueden mencionar firewalls, IDSs, honeypots, HIDS, etc.

Estas herramientas proveen información valiosa que, si no es tratada adecuadamente, puede fácilmente saturar la capacidad de interpretación del administrador encargado de la seguridad.

Un ejemplo de ello, es el caso de un sistema de detección de intrusos, en el cual podemos llegar a observar una gran cantidad de alertas, de las cuales la mayor parte son falsos positivos. Por otro lado, si optimizamos la capacidad de detección con el fin de disminuir la cantidad de falsos positivos, podemos caer en el problema de los falsos negativos, es decir que ocurra un evento y no lo hallamos detectado.

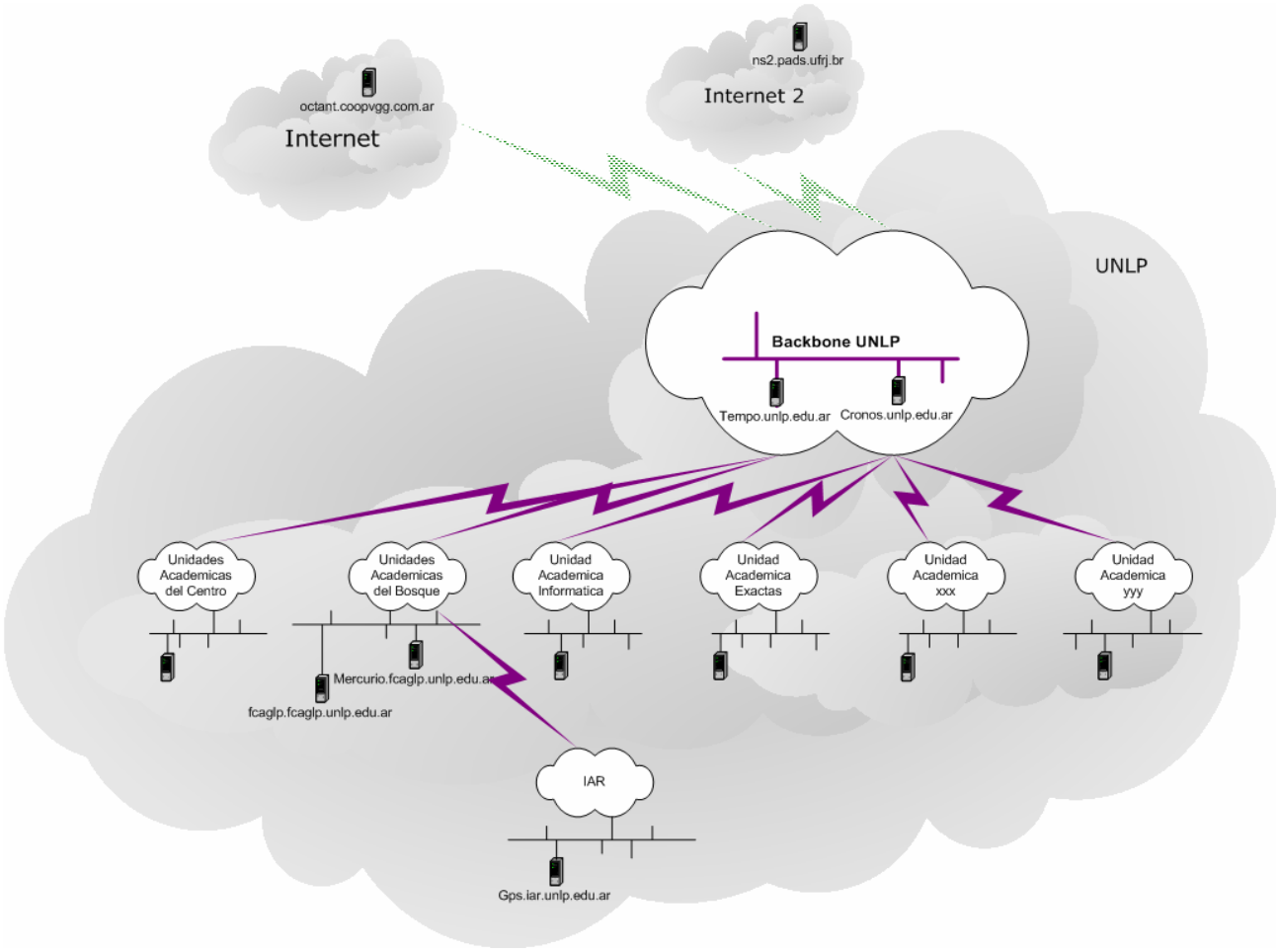
Otro ejemplo que podemos dar es cuando un honeypot no es el destino del ataque, caso en el cual la información registrada no es de utilidad.

Este trabajo propone la evaluación de diversas herrramientas de seguridad para la conformación y puesta a punto de una arquitectura de sensores distribuida que permita la centralización de la información recolectada para el posterior análisis y correlación, de modo de maximizar la confiabilidad de las alertas generadas. Se utilizará la red de la Universidad Nacional de La Plata para la implantación de dicha arquitectura.

Arquitectura de sensores de seguridad

Uno de los primeros requisitos para establecer una arquitectura distribuida es la sincronización de relojes. Para tal fin, se utilizó el protocolo NTP [Ref.1], el cual es un estándar reconocido para la sincronización de relojes en Internet. Se montó una arquitectura de servidores de tiempo, cuyo servidor central que brinda la hora oficial para la U.N.L.P. está ubicado en el core de la red y toma la hora de referencia del reloj del IAR [Ref.2], el cual es un reloj Stratum 0 de tipo GPS. Mecanismos de redundancia de relojes de referencia vía Internet e Internet2 fueron tomados para afrontar posibles cortes de disponibilidad que pueda haber con la red del IAR.

La siguiente figura muestra la arquitectura de relojes establecida para la sincronización.



Respecto a los sensores, se utilizaran distintas herramientas con el fin de recolectar información. Actualmente, han sido probadas las siguientes:

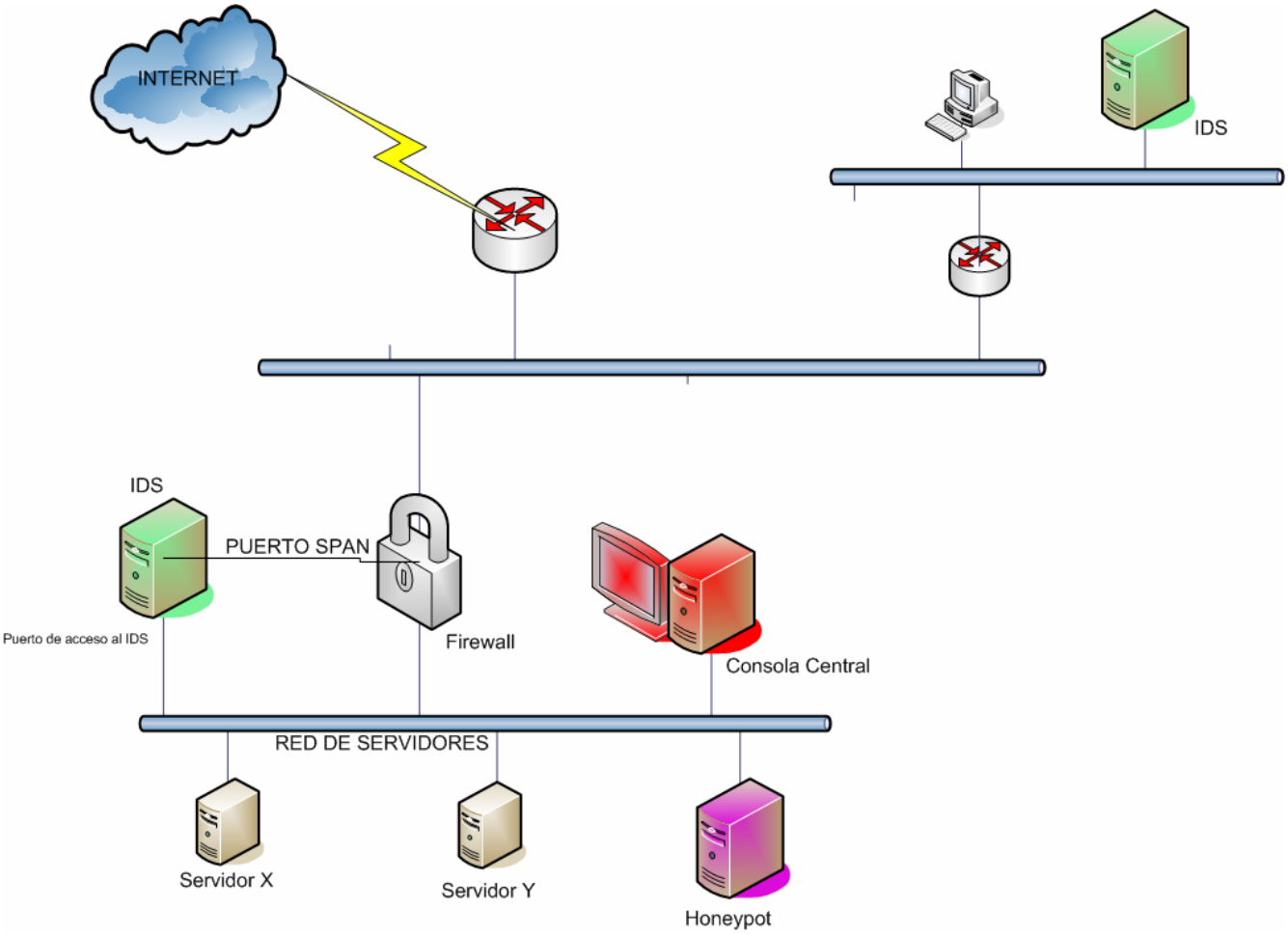
- SNORT [Ref.3]: es el sensor de red de facto del mercado en materia de IDSs. Se lo usa en forma distribuída en diferentes lugares de la red en forma no promiscua. En el caso de redes de servidores con muchas restricciones de seguridad se lo utiliza en forma promiscua, conectados a un puerto de SPAN en el que se replica el todo el tráfico del segmento protegido.
- PF [Ref.4]: En nuestra organización se usa el PF (Packet filter) que es el firewall de OpenBSD. Se utiliza OpenBSD en una configuración transparente de bridge, con una política de firewall restrictiva, la cual loguea todo el tráfico denegado que se genera en forma interna, es decir proveniente de los servidores que se protegen. Cualquier alerta del firewall, por su ubicación implica un profundo análisis del alerta generado porque puede reflejar el compromiso de un servidor.
- Syslog: Por medio de un servidor de logs se pueden exportar los mensajes de diferentes dispositivos a la consola central. Esta aplicación ha sido testeada con logs de routers Cisco y con logs de servidores.

A futuro se probaran las siguientes:

- Honeyd, integrandolo como honeypots a la arquitectura de sensores.

- Mwcollect/nepenthes como colectores de mallwar.
- SAMHAIN como chequeadores de integridad del filesystem del servidor en el que corra.
- SANCP [Ref.5] como analizador estadístico del tráfico de red, el cual permite detectar patrones anormales en el tráfico por medio de una serie de reglas
- Nessus como escaneadores de vulnerabilidades
- Iptables como firewall de Linux.

Para la tarea de centralización de la información, se evaluaron 2 aproximaciones, OSSIM [Ref.6] y Prelude [Ref.7]. Se eligió Prelude para la implementación de la arquitectura distribuida porque tiene una mejor escalabilidad en la conformación de la arquitectura distribuida, maneja un formato estándar de mensajes estándar, llamado IDMEF [Ref.8] (Intrusion Detection Message Exchange Format) y además por la creciente cantidad de herramientas opensource que interactuar con esta herramienta.



Sin embargo no se niegan las capacidades de OSSIM para el manejo de la información de seguridad y su posterior correlación. Es por ésto que OSSIM será utilizado como referencia con el objeto de comparar la información obtenida en ambos sistemas.

Finalmente, debemos mencionar que la correlación de datos, el punto crucial de la arquitectura, está en desarrollo. Desde el propio producto Prelude, se tuvieron dos iniciativas para correlacionar los datos. La primera de ellas se basó en el producto OpenSource SEC [Ref.9], "Simple Event Correlator", el cual permitió detectar un número limitado de ataques como ser propagación de gusanos, ataque de fuerza bruta y usuarios generando cantidades excesivas de trafico. La segunda de ellas, la que actualmente están desarrollando, está basada en la primera, extendiendo sus capacidades. De todas formas, más allá que Prelude provea una aproximación al tema de la correlación, no se descartan técnicas propias para la correlación de los mismos.
Será necesario evaluar las técnicas de correlación analizando el impacto respecto de la certeza de las alertas generadas como así también de la certeza de la omisión de las mismas.

Conclusiones

La implementación de una arquitectura de sensores de seguridad distribuida permitirá mejorar la calidad de las alertas generadas, incrementando su confiabilidad. Además la información recolectada y correlacionada puede ser usada en cualquier grupo de seguridad de cualquier organización, posibilitando la detección temprana y la implementación de medidas proactivas ante incidentes de seguridad.

Otra línea de trabajo futura relacionada con el presente trabajo es la de la evaluación de la información recolectada localmente por esta arquitectura, frente a las amenazas de seguridad registradas a nivel internacional, como ser las generadas por el sitio www.dshield.org el cual es patrocinado por SANS.

Referencias

[Ref.1] http:// www.ntp.org
[Ref.2] http://www.iar.unlp.edu.ar/
[Ref.3] http://www.snort.org/
[Ref.4] http://www.openbsd.org/faq/pf/
[Ref.5] http://www.metre.net/sancp.html
[Ref.6] http://www.ossim.net
[Ref.7] http://www.prelude-ids.org
[Ref.8] http://www.rfc-editor.org/rfc/rfc4765.txt
[Ref.9] http://www.estpak.ee/~risto/sec/