Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Detector de ataques en Red basado en Software Libre

(snort + acidlab)

Hugo Francisco González Robledo
Departamento de Posgrado / Centro de Telecomunicaciones
Instituto Tecnológico de San Luis Potosí

hugo@honeynet.org.mx
hugo.gonzalez@itslp.edu.mx

Quién les habla

- M. C. en Ciencias de la Computación por el ITSLP.
- Participante en el Departamento de Posgrado.
- Más de 7 años de experiencia en uso de SL y más de 4 a nivel Profesional.
- NetAdmin. Migrando a Linux y OpenBSD. Y manteniendo Solaris.
- Ponente en diversos eventos.
- ITSLPixx

Agenda

- Introducción
- El problema
- Propuesta de solución
- Manos a la obra
- Conclusiones
- Sesión de Preguntas

Introducción

- En la actualidad la seguridad informática y la de red es un factor clave y fundamental
- La detección de intrusos va tomando cada día mayor auge, el uso de firewalls es “obligatorio”
- Los conocimientos necesarios de los atacantes cada vez son menores, y el tiempo en preparar y desarrollar un ataque se van reduciendo.

- grafica de ataques ....

El detector de ataques

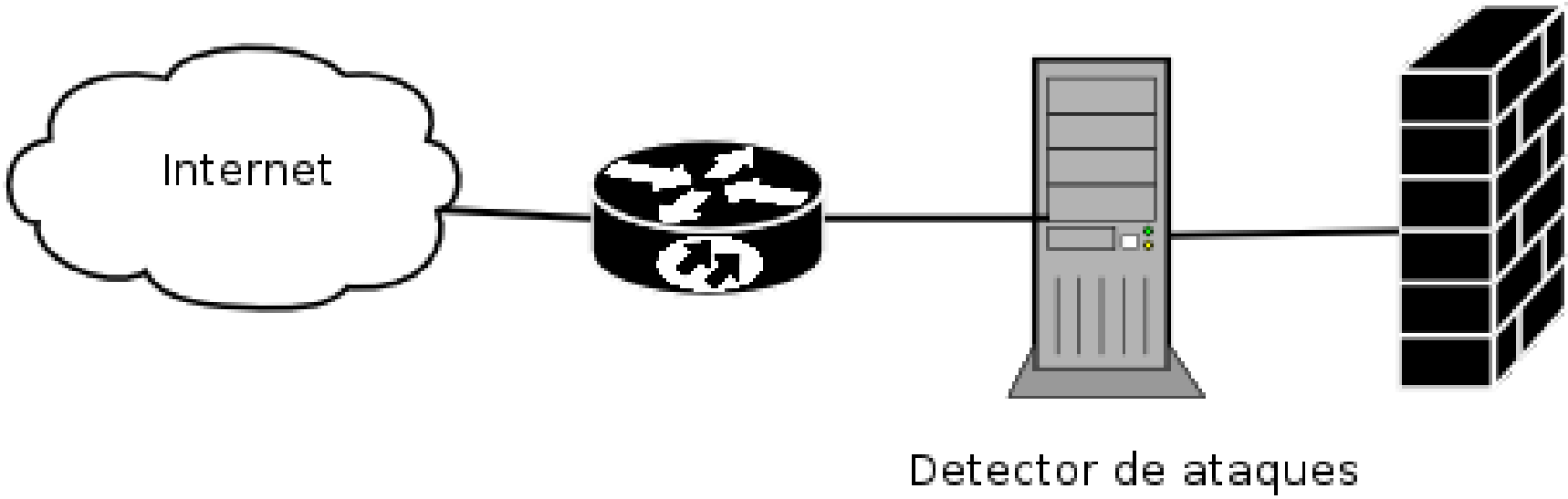
- Esta presentación se enfoca al detector de ataques, aunque puede servir como introducción a la detección de intrusos.

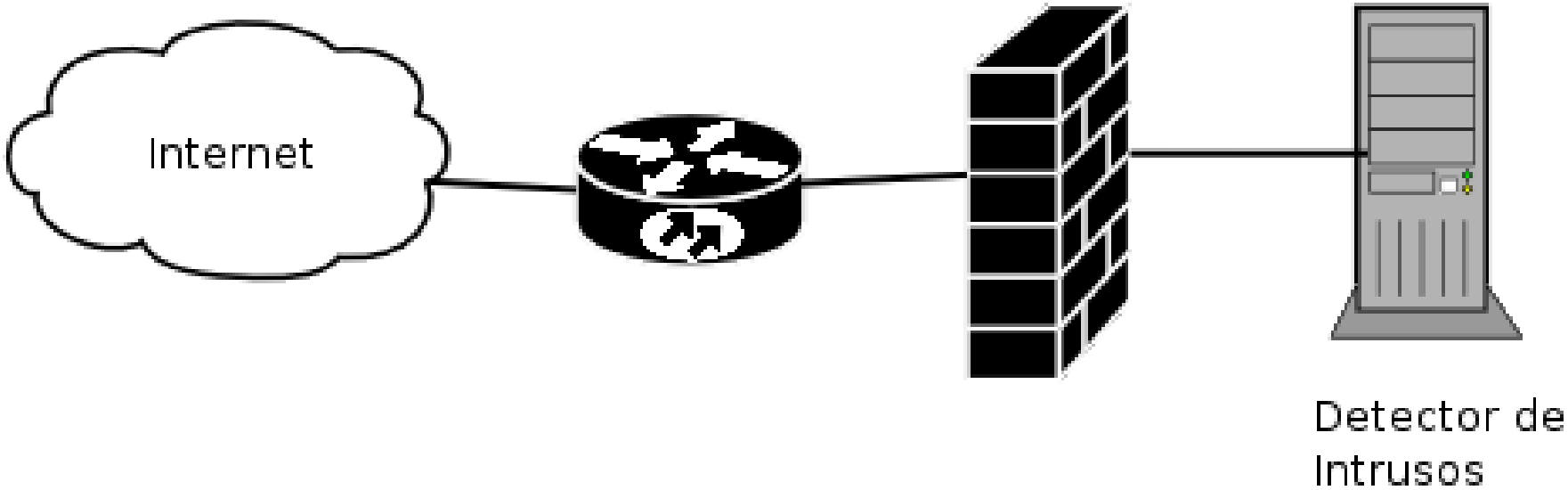
El problema

- ¿Cómo justificar las inversiones en TI?
- ¿Cómo justificar las inversiones en Seguridad?
- ¿Cómo justificar las inversiones en Personal?
- ¿Cómo justificar las inversiones en Capacitación?

Propuesta de Solución

- Aun cuando contemos con un firewall y un IDS, no siempre se comportan como esperamos.
- Existen diversas soluciones propietarias, y también de Free an Open Source Software. (FOSS)
- Detectar los ataques a nuestra red, independientemente de las tecnologías que se esten utilizando ya para protegerla.


Internet
Detector de ataques


Internet
Detector de
Intrusos

El detector de intrusos

- Existen a 2 niveles
  - de Host (HIDS)
  - de red (NIDS)
- Basados en firmas, o en heurísticas
- El estándar de Facto es snort (open source)
- Si no está actualizado no sirve ...

Prevención de Intrusos

- Existen añadidos para “prevenir” intrusiones
- Generalmente modifican las cadenas de entrada para minimizar daños
- Snort-inline
-
-
- Ejemplos :.....

Detector de Ataques

- Directamente en Internet
- Fuera de cualquier dispositivo de seguridad
- Fácil administración, mantenimiento
- Seguro
- “Transparente”

Manos a la obra

- Necesitamos ...
- Linux o cualquier otro sabor de *NIX
- SNORT
- ACID (se puede utilizar BASE)
- es necesario PHP, MySQL, APACHE ... (como complemento)
- Recomiendo DEBIAN o cualquier derivado como UBUNTU

Instalándolo en DEBIAN

- recurrimos al fabuloso “apt-get”
- apt-get install snort
- apt-get install acidlab
-
- La configuración se va realizando junto con la instalación (gracias DEBIAN ;))

200.36.36.120 - PuTTY

Configuración de Debian

Configuración de snort-mysql

Por favor, introduzca el nombre de la interfaz en la que Snort debe escuchar. Puede obtener los nombres de las interfaces ejecutando «ip link show». Este valor suele ser «eth0», pero quizás desee variarlo dependiendo de su entorno. Si está utilizando una conexión de teléfono mediante PPP a Internet puede ser más apropiado utilizar «ppp0».

Tenga en cuenta que generalmente se configura a Snort para que analice todo el tráfico que viene de Internet, así que la interfaz que se añade aquí es generalmente la misma que tiene definida la ruta por omisión. Para determinar qué interfaz se está utilizando para esto, ejecute bien «ip route show» o bien «/sbin/route -n» (busque aquellos valores asociados a «default» o «0.0.0.0»).

Tampoco es infrecuente ejecutar Snort en una interfaz sin dirección IP

<Aceptar>

200.36.36.120 - PuTTY

Configuración de Debian

Configuración de snort-mysql

¿En qué interfaz debería escuchar Snort?

eth0

<Aceptar>

Configuración de Debian

Configuración de acidlab

ACIDlab supports any web server that php3/php4 does, but this automatic configuration process only supports Apache and Apache-SSL.

Which web server would you like to reconfigure automatically?

- Apache
- Apache-SSL
- Both
- None

<Aceptar>

200.36.36.120 - PuTTY

Configuración de Debian

Configuración de acidlab

Which host does your alert database reside on?

Alert database hostname

localhost

<Aceptar>

200.36.36.120 - PuTTY

Configuración de Debian

Configuración de acidlab

What password should be used when connecting to the archive database?

Archive database password

****

<Aceptar>

Analysis Console for Intrusion Databases (ACID) - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

http://ardilla.zapto.org/acidlab/acid_main.php

Ir welsh

Getting Started Latest Headlines Diccionario

Curso de Perl - Capítulo 3 | intelligence: Volume 12, Is... | Alan Cox - Wikipedia, the ... | O'Reilly Network: The Nex... | Hakin9 Official Web Site | Analysis Console for I...

Analysis Console for Intrusion Databases

The underlying database snortacid@localhost appears to be incomplete/invalid.

The database version is valid, but the ACID DB structure (table: acid_ag) is not present. Use the **Setup page** to configure and optimize the DB.

Buscar: welsh Buscar siguiente Buscar anterior Resaltar Coincidir mayúsculas

Listo

ACID: DB Setup - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

http://ardilla.zapto.org/acidlab/acid_db_setup.php

Getting Started Latest Headlines Diccionario

Curso de Perl - Capítulo 3 | intelligence: Volume 12, Is... | Alan Cox - Wikipedia, the ... | O'Reilly Network: The Nex... | Hakin9 Official Web Site | ACID: DB Setup

ACID

DB Setup

Home
Search | AG Maintenance

[Back]

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	Create ACID AG
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

[Loaded in 0 seconds]

ACID v0.9.6b20-5.1 (by **Roman Danyliw** as part of the **AirCERT** project)

Buscar: welsh Buscar siguiente Buscar anterior Resaltar Coincidir mayúsculas

Listo

ACID: DB Setup - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

http://ardilla.zapto.org/acidlab/acid_db_setup.php

Getting Started | Latest Headlines | Diccionario

Curso de Perl - Capítulo 3 | intelligence: Volume 12, Is... | Alan Cox - Wikipedia, the ... | O'Reilly Network: The Nex... | Hakin9 Official Web Site | ACID: DB Setup

ACID

DB Setup

Home
Search | AG Maintenance

[Back]

Successfully created 'acid_ag'

Successfully created 'acid_ag_alert'

Successfully created 'acid_ip_cache'

Successfully created 'acid_event'

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	DONE
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

The underlying Alert DB is configured for usage with ACID.

Additional DB permissions
In order to support Alert purging (the selective ability to permanently delete alerts from the database) and DNS/whois lookup caching, the DB user "snort" must have the DELETE and UPDATE privilege on the database "snortacid@localhost"

Goto the **Main page** to use the application.

[Loaded in 1 seconds]

ACID v0.9.6b20-5.1 (by **Roman Danyliw** as part of the **AirCERT** project)

Buscar: welsh | Buscar siguiente | Buscar anterior | Resaltar | Coincidir mayúsculas

Listo

Analysis Console for Intrusion Databases (ACID) - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

http://ardilla.zapto.org/acidlab/acid_main.php

Getting Started Latest Headlines Diccionario

Curso de Perl - Capítulo 3 | intelligence: Volume 12, Is... | Alan Cox - Wikipedia, the ... | O'Reilly Network: The Nex... | Hakin9 Official Web Site | Analysis Console for I...

Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queried on : Tue September 13, 2005 21:03:11
Database: snortacid@localhost (**schema version:** 106)
Time window: [2005-09-13 21:02:50] - [2005-09-13 21:02:51]

Sensors: 1
Unique Alerts: 4 (2 **categories**)
Total Number of Alerts: 7

- Source IP addresses: 1
- Dest. IP addresses: 1
- Unique IP links 3

- Source Ports: 1
  - TCP (1) UDP (0)
- Dest. Ports: 1
  - TCP (1) UDP (0)

Traffic Profile by Protocol

TCP (50%)

UDP (0%)

ICMP (50%)

Portscan Traffic (0%)

- Search
- Graph Alert data

- **Snapshot**
  - Most recent Alerts: **any protocol**, **TCP**, **UDP**, **ICMP**
  - Today's: alerts **unique**, **listing**; IP **src** / **dst**
  - Last 24 Hours: alerts **unique**, **listing**; IP **src** / **dst**
  - Last 72 Hours: alerts **unique**, **listing**; IP **src** / **dst**
  - Most **recent 15 Unique Alerts**

  - Last Source Ports: **any** , **TCP** , **UDP**

  - Most **frequent 5 Alerts**

  - Most Frequent Source Ports: **any** , **TCP** , **UDP**
  - Most Frequent Destination Ports: **any** , **TCP** , **UDP**

  - Most frequent 15 addresses: **source**, **destination**

Buscar: welsh Buscar siguiente Buscar anterior Resaltar Coincidir mayúsculas

Listo

Experiencias

- La base de datos de MySQL crece y crece, y crece, y crece .....
- Se me llenó un disco de 2 Gb :)
- Una mala configuración genera mucha “basura”
- Puede generar confusión

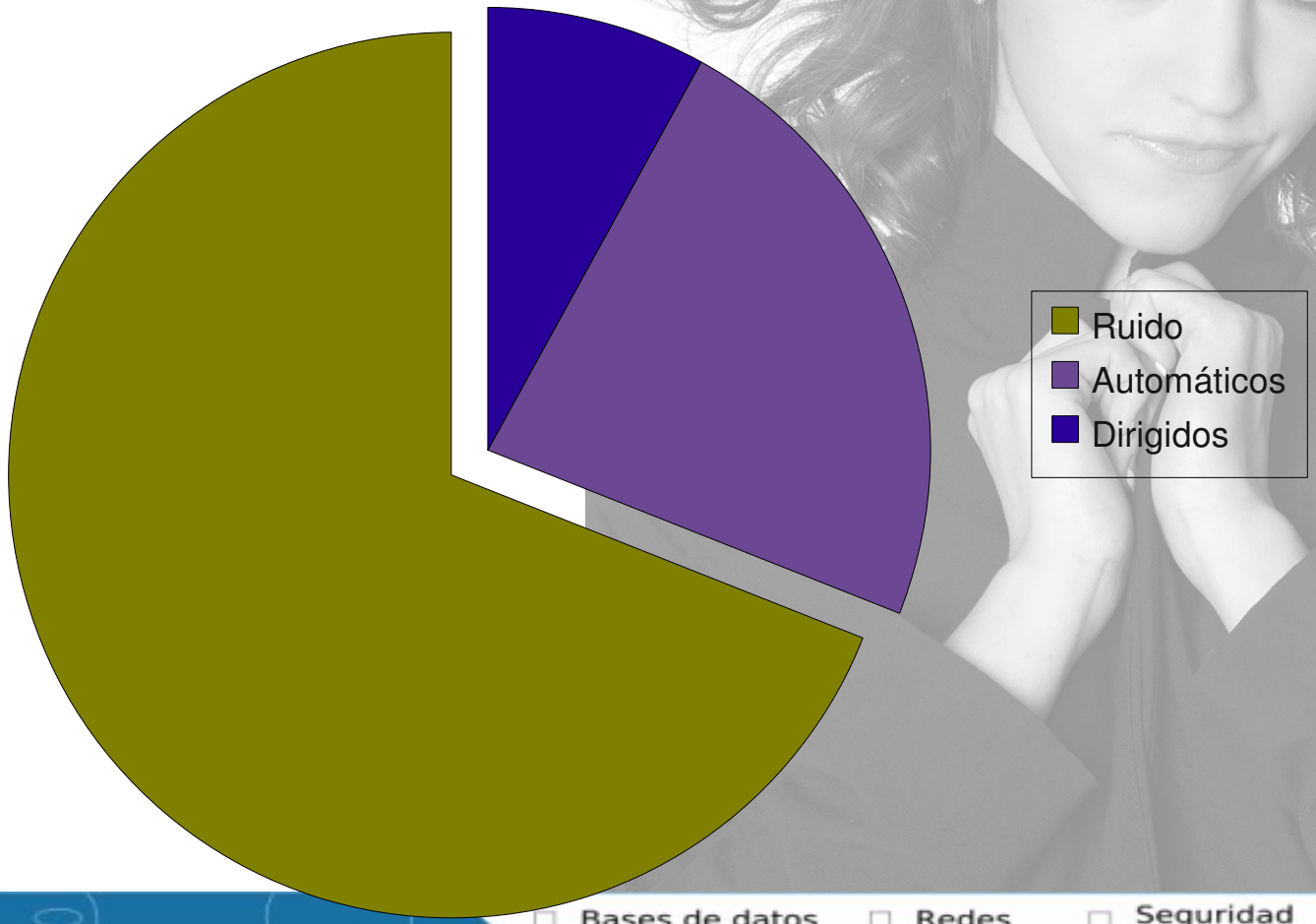
Ejemplo, el detector en el ITSLP

Conclusiones

- Las soluciones open source nos brindan mucha mayor flexibilidad.
- Podemos ofrecer una visión global de la situación de nuestra red (o equipo)
- Las inversiones en TI se pueden justificar, mostrando los niveles y tipos de ataques que se generan

Gráficas

Clasificación



Trabajo a futuro

- Migrar de acidlab a acidbase
- Distribuir los detectores
- Utilizar tecnologías P2P para controlar y comunicar los clientes
- Optimizar la base de datos y eliminar la información antigua

Agradecimientos

- Al ITSLP :
  - Centro de cómputo por dejarme jugar con las máquinas
  - Posgrado por el apoyo para el viaje
- MHP
- Organizadores del evento
  - Por la invitación
- La comunidad FOSS ...

Preguntas !

- GRACIAS !
-
- http://www.itslp.edu.mx
- http://www.honeynet.org.mx
- http://ardilla.zapto.org
- http://ardilla.zapto.org/presentaciones/
-
- hugo.gonzalez@itslp.edu.mx
- hugo@honeynet.org.mx