

# **This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.**

To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>



**Hugo González**



**@hugo\_glez**

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

# The Honeynet

P R O J E C T

Montando una honeynet  
CONSOL 2007

Hugo F. González  
hugo@honeynet.org.mx

# ¿ Quién les habla ?

- Miembro fundador del “Mexican Honeynet Project”, miembro profesional de ACM desde 2005.
- M.C. por el ITSLP en 2005.
- Asesor académico en la UPSLP.
- Usuario de SL desde hace mas de 7 años.
- Conferencista en eventos nacionales e internacionales.



# Agenda

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



# Introducción

- El estado de la seguridad en Internet es pobre
- Cualquiera puede ser un objetivo (virus, botnets ...)
- Los atacantes cada vez requieren menos conocimientos, existen muchas herramientas para ataques automáticos



# Conoce a tu enemigo

- Atacantes o “black hats”
  - ¿Quienes son ?
  - ¿Qué herramientas utilizan?
  - ¿Por qué me atacan?



# ¿Qué es un Honeypot?

- A honeypot is a resource that is intended to be probed, attacked, or compromised. (Lance Spitzner)
- “A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource”, (Lance Spitzner)
- “A honeypot is a fictitious vulnerable IT system used for the purpose of being attacked, probed, exploited and compromised.” (Piller/Wolfgarten)



# ¿Qué es una honeynet?

- Un tipo de honeypots
- Pueden estar en un mismo equipo (virtualización) o en diversos equipos.
- Honeywall + honeypots
- Diferentes o iguales sistemas operativos
- Incluso de dispositivos ... como routers, wireless, BD, etc.
- Todo el tráfico es sospechoso





# Baja Interacción

- Emulan servicios y sistemas operativos
  - Captura limitada de información
  - Riesgo bajo
- 
- kfsensors
  - specter
  - honeyd



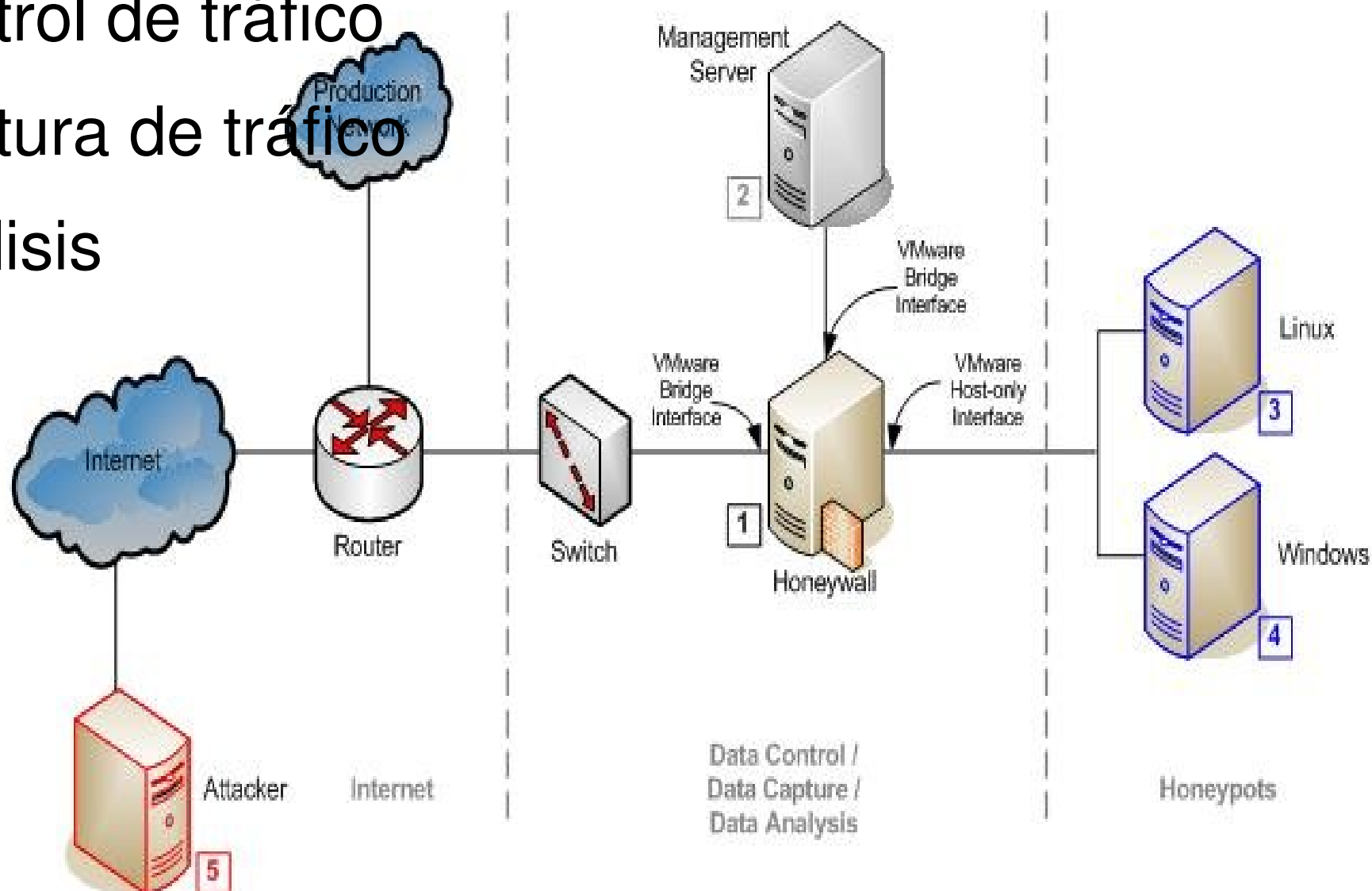
# Alta interacción

- Sistemas operativos completos, no se emulan
- Generalmente en instalaciones por defecto
- El atacante puede tomar el control completo del sistema
- Capturan mayor cantidad de información
- Mayor riesgo, complejos de implementar
- Linux
- Unix
- Win2k



# Honeynet Gen II

- Control de tráfico
- Captura de tráfico
- Análisis



# Riesgos

- El atacante sabe que es un honeypot
- El atacante toma control completo sobre el sistema, desactiva sebek ...
- Genera información falsa
- Es posible explotar un honeypot



# Y a todo esto ... ¿Para qué &%#\$&%\$ quiero uno?

- Aprender ??
- Distraer al atacante.
- Monitorear tus sistemas.
- Demostrar que hay gente interesada en tu red.
- Detectar malware
- Justificar gasto en seguridad informática
- Detectar nuevos ataques y zero-days



# Opciones para los clientes

- Propio
  - netcat ?
- honeyd, nephentes
  - baja interacción
  - sencillo, usable
- vmware, qemu
  - alta interacción
  - complejo



# Diseñando nuestro honeynet

- Objetivos del honeynet
  - ataques, virus, gusanos, spam
- Disponibilidad de direcciones
- Disponibilidad de equipos
- Cercano a nuestra red de producción
- “Nuestra red de producción”



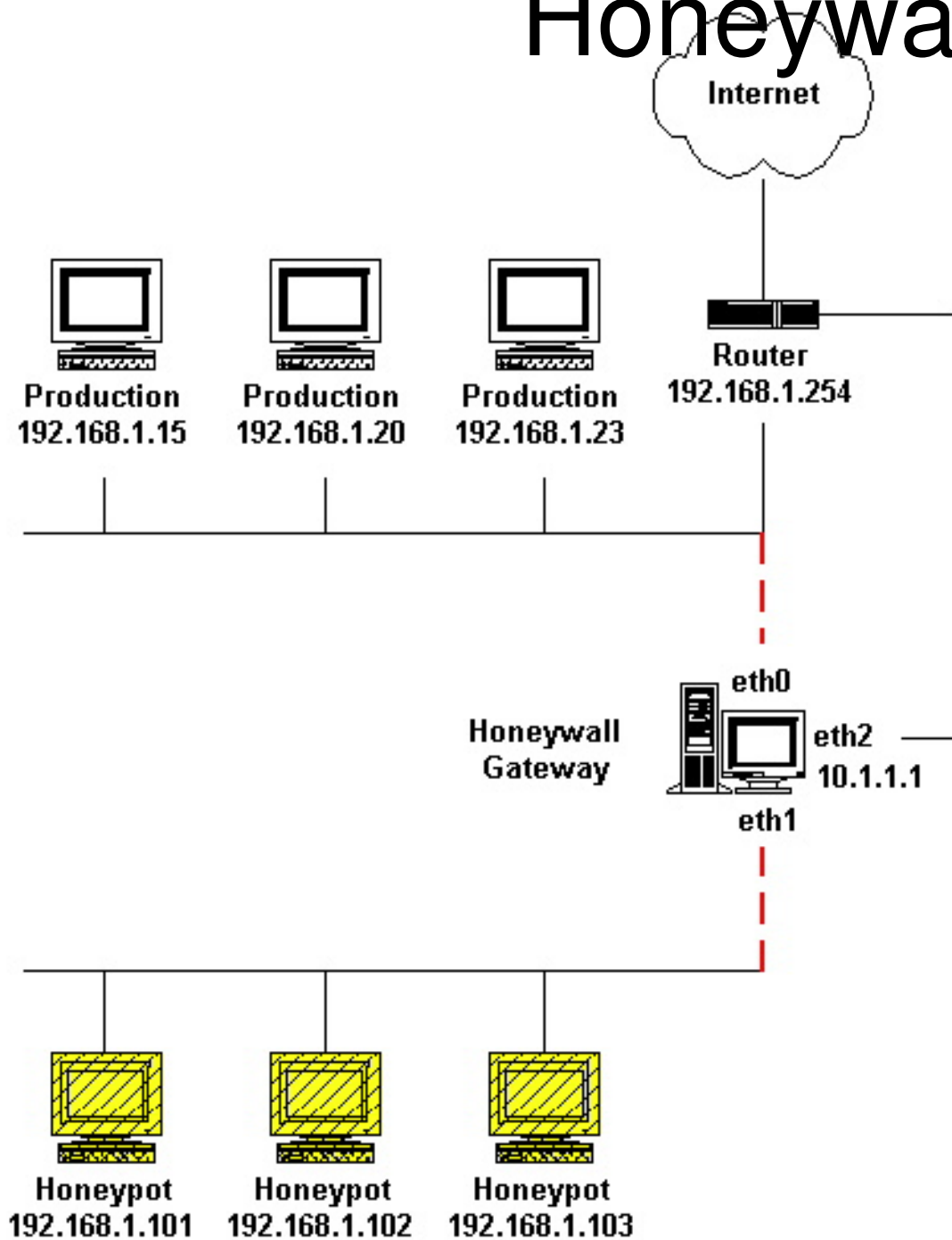
# Eligiendo la virtualización, o no

- Asistieron a “emulación con qemu”
- Excelente opción
- VMWare ????
- UML
- Virtuozzo
- Xen

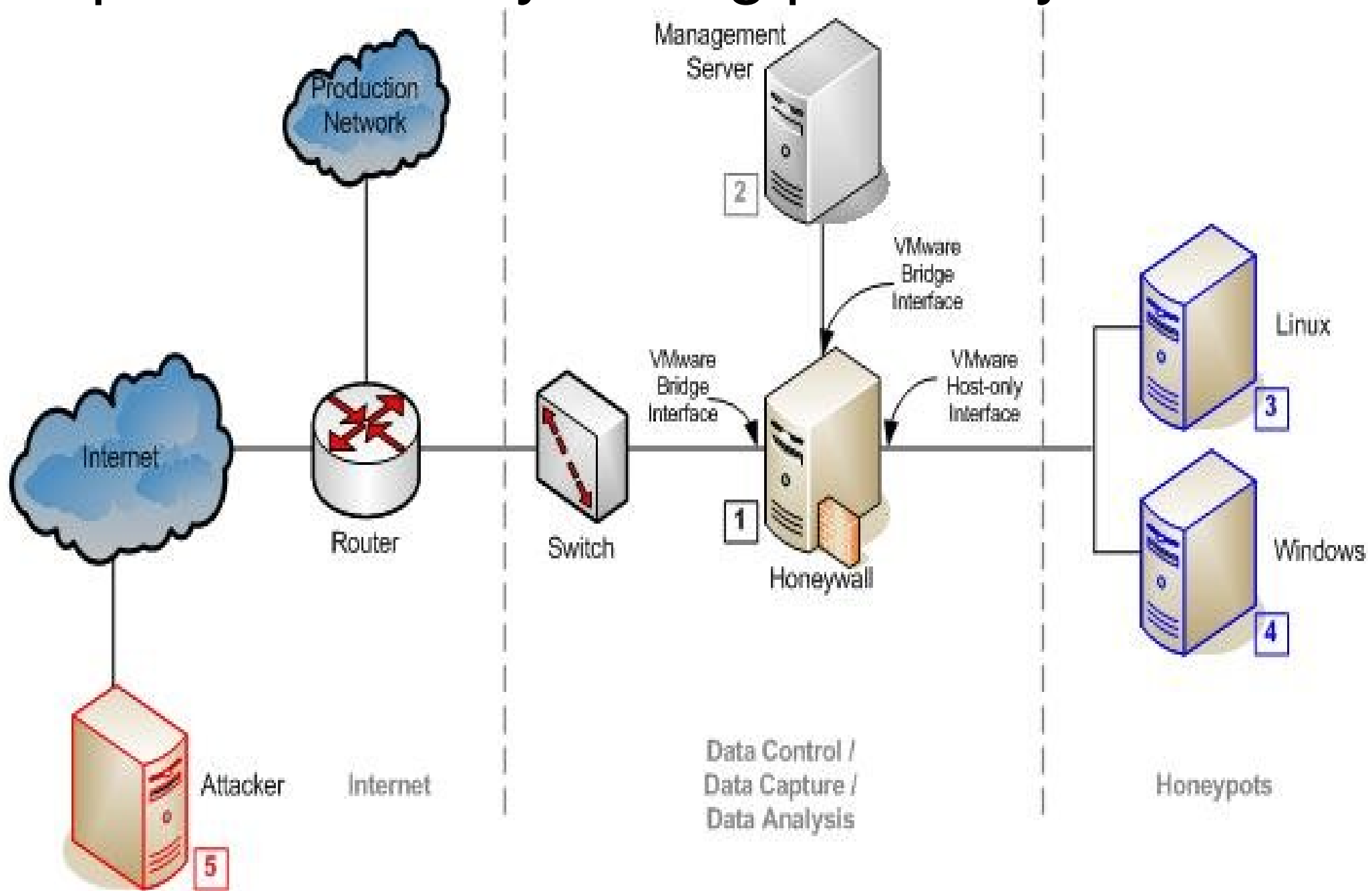




# Honeywall



<http://www.honeynet.org.pk/honeywall/roo/>



# Instalación de Honeywall

- Arrancar el equipo con el disco de honeywall dentro y darle aceptar.
- Es una instalación automática.
- Fedora Core 3 mínimo + herramientas para control, captura y análisis de datos.



# Configuración

- La primera vez te dice que no está configurado y te ofrece un asistente.
- La mejor opción para comenzar es eligiendo interview.
- Luego puedes ajustar la información a mano.



# Todo lo que hicimos lo montamos dentro de un debian corriendo qemu.

- qemu no se pueden conectarse directamente entre los equipos virtualizados.
- Se tiene que usar bridge para conectar el qemu con nuestra red
- 
- `qemu -hda disco -net nic -net tap ...`
- utilizar vde ...
- vde permite generar hub's y swithc virtuales



# Ya tengo la honeynet y luego ??

- Cuando un equipo es comprometido nos da bastante información para saber que ha estado pasando, de donde se conectaron y que es todo lo que se ha estado haciendo.
- Seebek nos da información a nivel kernel, acidlab y snort nos dan información sobre la red ...
- Podemos realizar una captura de tráfico de red y aplicar el análisis forense de red



# Análisis Forense de Red

1. Crear un nuevo directorio para el análisis.
2. Cambiar los permisos de los archivos como solo lectura.
3. Obtener las firmas hash de los archivos
4. (marcado como opcional) ejecutar capinfos para obtener datos estadísticos iniciales.
5. Ejecutar tcpdstat para obtener información estadística básica.



6. Ejecutar argus para extraer información de las sesiones
7. (opcional) Ejecutar Ragator en el archivo argus para conciliar datos de sesiones redundantes.
8. Ejecutar racount en el archivo argus para contar los registros de sesiones.
9. Ejecutar rahosts en archivo argus para observar todas las direcciones ip
10. Ejecutar ra en el archivo argus para enumerar las direcciones fuente y destino, y las combinaciones de puertos.





- 11. Ejecutar ra directamente para observar los datos de la sesion directamente
- 12. Ejecutar tcpflow para seguir conexiones de manera completa ...
- 13. (opcional) Ejecutar snort ...
- 14. (opcional) Ejetuar ethereal ... ahora si, con toda esta información de seguro encuentras lo que estas buscando.



# Nepenthes

- Es un honeypot de baja interacción
- Captura los “bichos” en internet, detecta el ataque, almacena el tráfico de la red, interactúa con el ataque y “baja” el código dañino, generalmente bot ...



# aranaia

- <http://code.google.com/p/arania>
- Para funcionar en servidores en producción
- Intenta detectar las inyecciones de código o ejecuciones remotas, baja el código y si existe un bot, también lo baja.



# Conclusiones

- Nuestro honeynet lista en menos de una hora.
- Honeypot es una herramienta muy útil para aprender
- Honeynet multiplicas las oportunidades, pero también el trabajo.
- No es suficiente poner la honeynet, hay que monitorearla y aprovechar la información que se obtiene.
- Las herramientas están ahí, y en su mayoría son open source, aprovechemoslas.



# Trabajo a futuro

- Poner mas honeypots y honeynets ...
- Investigar sobre ataques, virus y gusanos.
- Compartir las lecciones aprendidas.



# Agradecimientos

- AI ITSLP :
  - Centro de cómputo por dejarme jugar con las máquinas
- Universidad Politécnica de San Luis Potosí por el apoyo para el viaje
- MHP
- Organizadores del evento
  - Por la invitación
- La comunidad FOSS ...



# Referencias

- Debian GNU/Linux
  - [www.debian.org](http://www.debian.org)
  - [www.debian.org.mx](http://www.debian.org.mx)
- Honeynet
  - [www.honeynet.org](http://www.honeynet.org)
  - [www.honeynet.org.mx](http://www.honeynet.org.mx)



# ¿ Preguntas ?

GRACIAS !

<http://www.upslp.edu.mx>

<http://www.honeynet.org.mx>

<http://ardilla.zapto.org>

<http://ardilla.zapto.org/presentaciones/>

[hugo.gonzalez@upslp.edu.mx](mailto:hugo.gonzalez@upslp.edu.mx)

[hugo@honeynet.org.mx](mailto:hugo@honeynet.org.mx)

