

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/>

Honeynet en menos de una hora



Hugo Francisco González Robledo

Departamento de Posgrado

Instituto Tecnológico de San Luis Potosí

Mexican Honeynet Project

hugo.gonzalez@itslp.edu.mx

hugo@honeynet.org.mx

<http://ardilla.zapto.org>, <http://www.honeynet.org.mx>



CICOL 2006

- ☐ Bases de datos
- ☐ Redes
- ☐ Seguridad
- ☐ Programación
- ☐ Software Libre

¿ 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.



Agenda

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





Introducción



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?



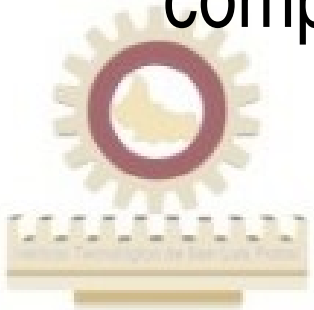
El primer “Honeypot”

- Kevin D. Mitnick
 - El “hacker” más famoso por ser perseguido por la justicia.
- Shimomura
 - Lo atrapa con una especie de “Honeypot”
 - Un equipo tentador para Mitnick, y almacena toda la evidencia.



¿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.
- Representan toda una red ...
- 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



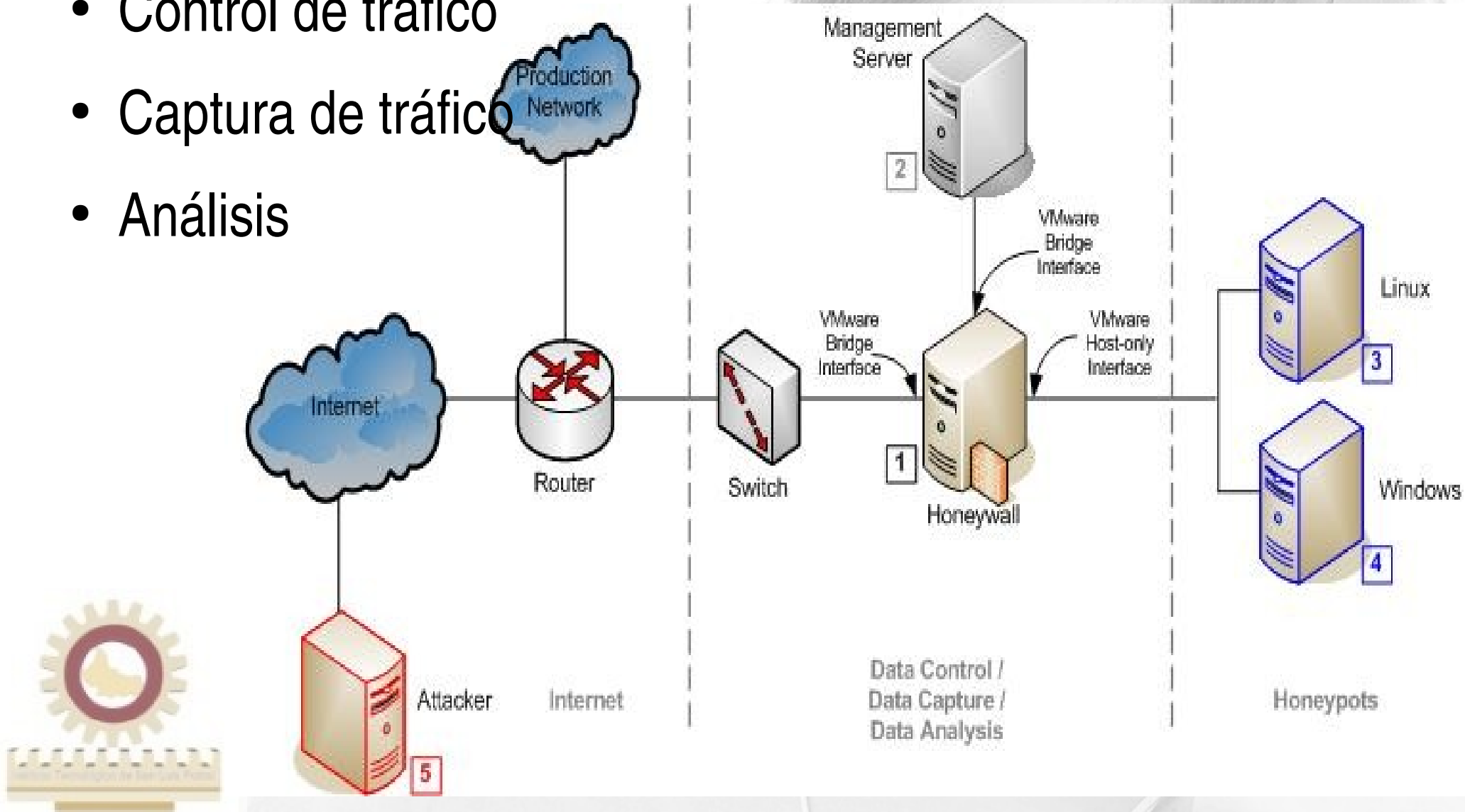
Alta interacción

- 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



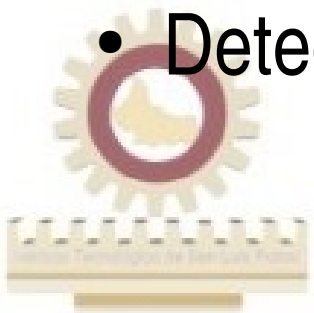
Riesgos

- 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



Mi caso

- Contamos con un detector de Ataques en Red (snort+ACID)
- Monitorear que más quieren ...
- Detectar virus, troyanos y malware en la red
- Detectar “jóvenes inquietos” (insider attackers)
- Justificar inversión



Opciones para los clientes

- Propio
 - netcat ?
- honeyd
 - baja interacción
 - sencillo, usable
- vmware, qemu, virtualización de Solaris
 - alta interacción
 - complejo
 - La virtualización solo permite sistemas Solaris





Manos a la obra



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”

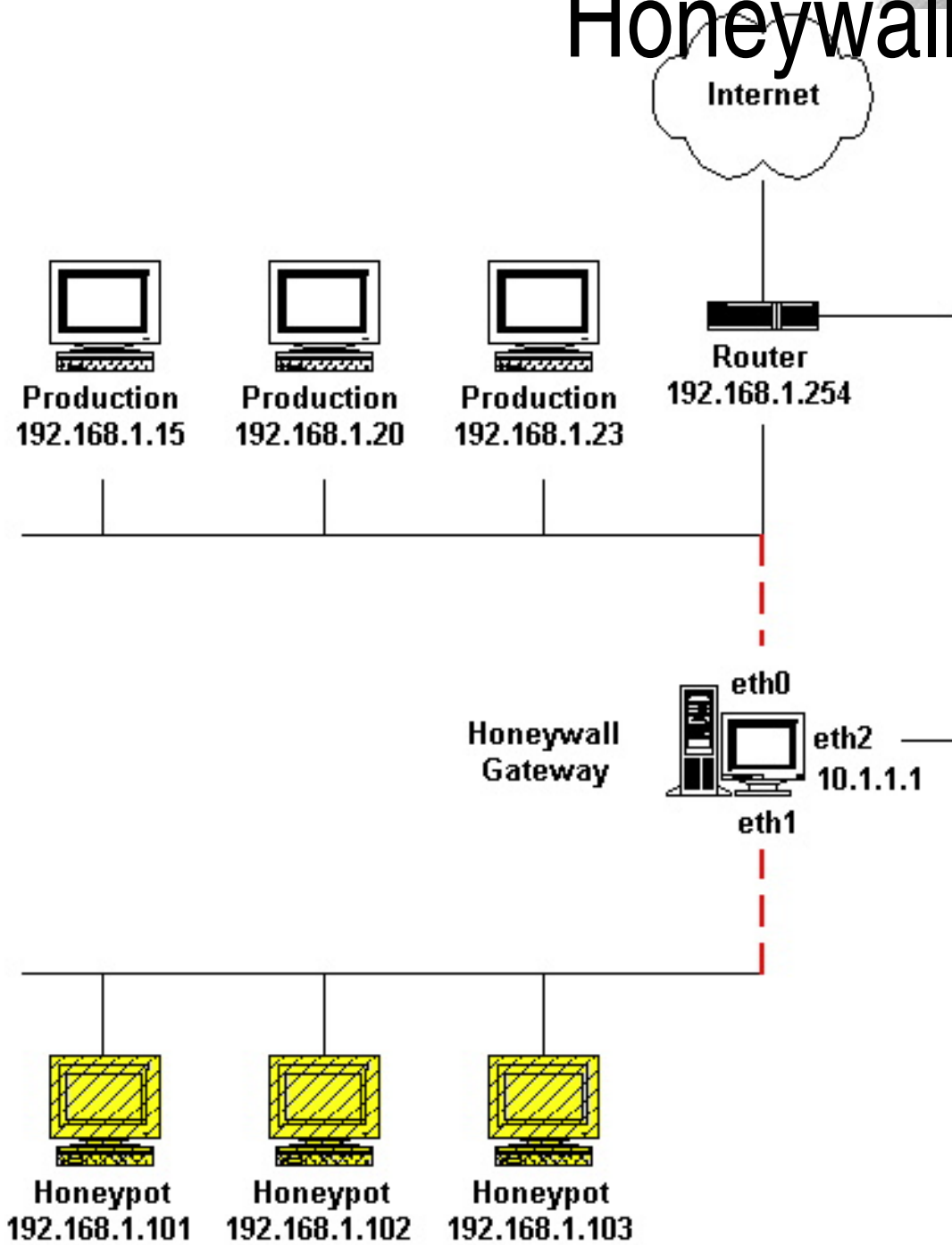


Eligiendo la virtualización, o no

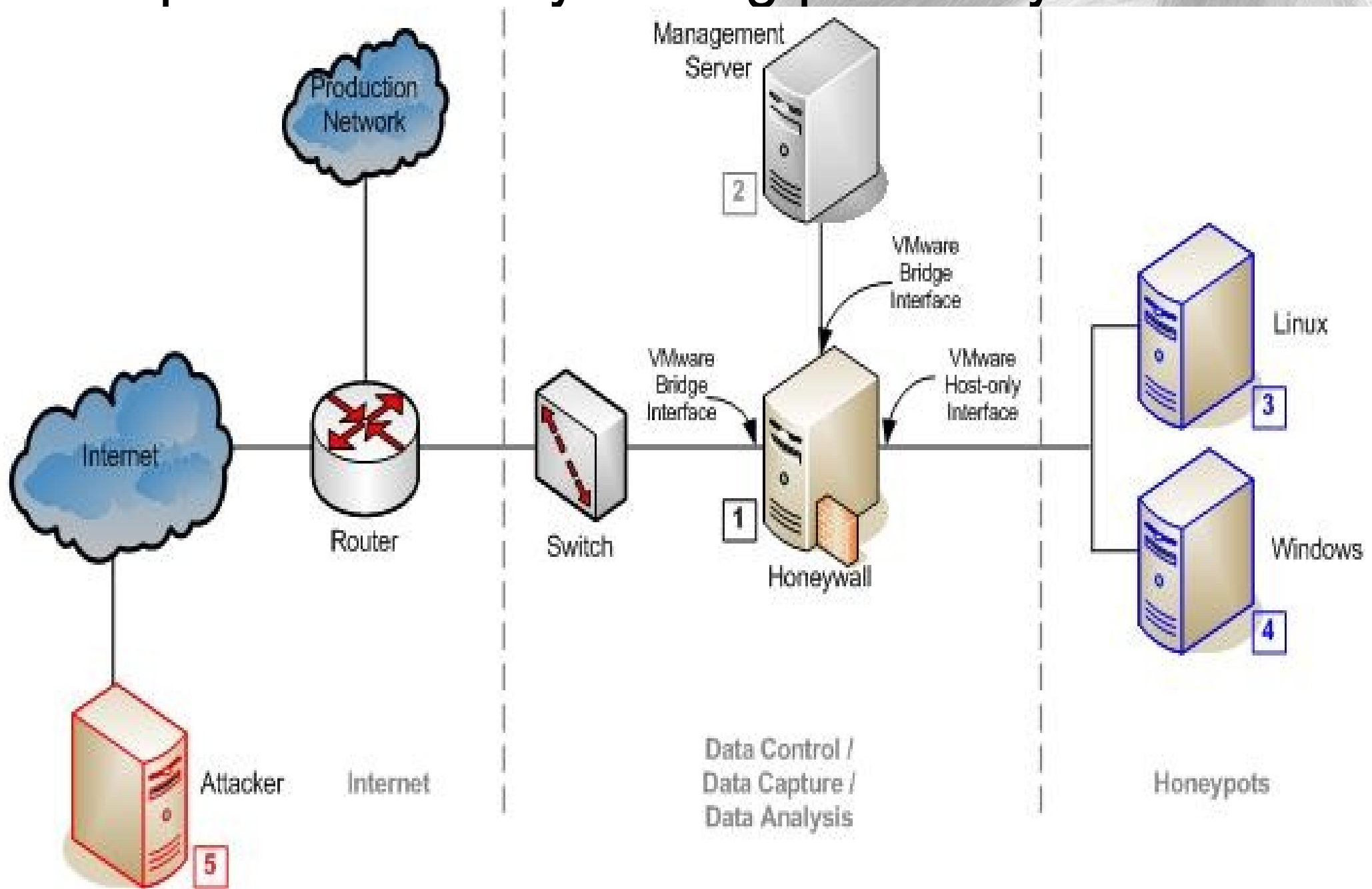
- Asistieron a “emulación con qemu”
- Excelente opción
- VMWare ????
- UML
- Virtuozzo
- Xen



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.



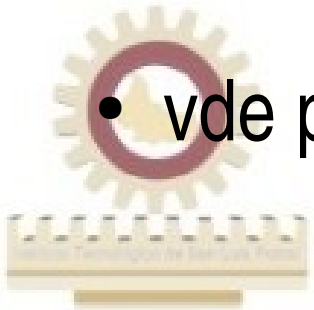
Configuración

- 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



Algunos datos del ITSLP

- Diversos intentos automáticos de explotación (a toda la red, no solo al honeynet)
- Hasta el día 25 de Junio de 2006 no se ha comprometido ninguna máquina.
- Ataque del ircbot energie.txt ...
- Ataque a Mambo y Joomla
- Más información próximamente ...



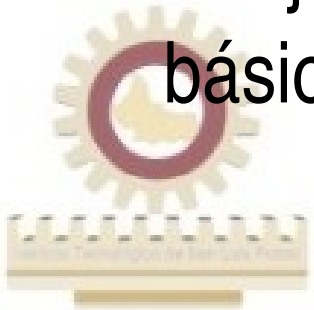
Ya tengo la honeynet y luego ??

- 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.





Conclusiones



Conclusiones

- Nuestro honeynet lista en menos de una hora.
- Honeybot 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.
- Unir esfuerzos con el MHP.



Trabajo a futuro

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



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 ...



Referencias

- Debian GNU/Linux
 - www.debian.org
 - www.debian.org.mx
- Honeynet
 - www.honeynet.org
 - www.honeynet.org.mx
- Qemu





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

