Hugo González

@hugo_glez

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

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Honeynet en menos de una hora

Hugo Francisco González Robledo

Universidad Politécnica de San Luis Potosí
Mexican Honeynet Project
hugo.gonzalez@upslp.edu.mx
hugo@honeynet.org.mx
http://ardilla.zapto.org, http://www.honeynet.org.mx

6tas. Jornadas Regionales de Software Libre

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Octubre 14, 2006. Mendoza, Arg.

Jornadas Regionales de 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.
- ITSLPixx

Agenda

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Introducción

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Conoce a tu enemigo

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

¿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)

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

¿Qué es una honeynet?

- Un tipo de honeypot
- Todo el tráfico es sospechoso
- Herramienta
- Existen varias generaciones

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Baja Interacción

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

- kfsensors
- specter
- honeyd

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

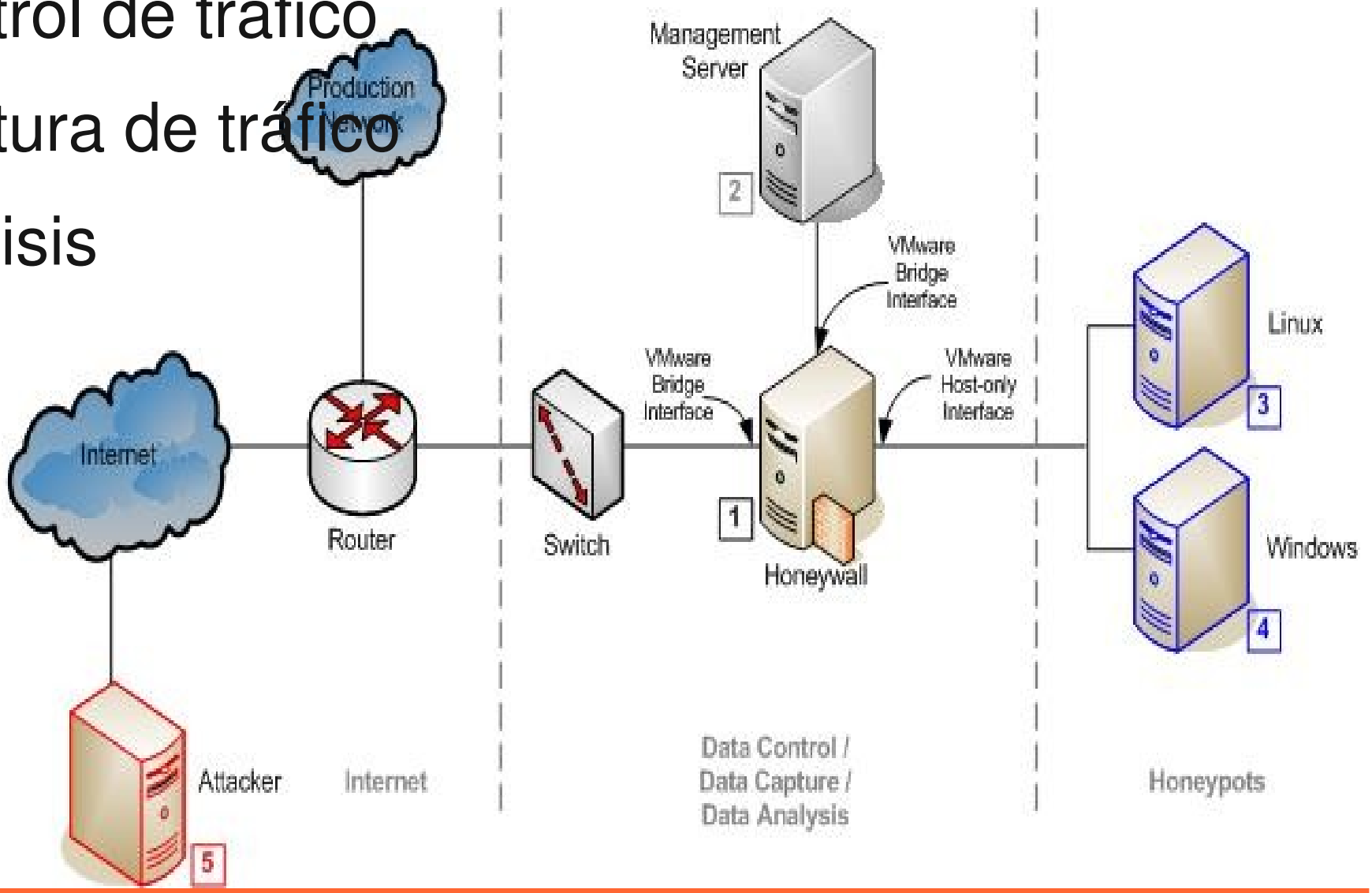
Alta interacción

- 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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Honeynet Gen II

- Control de tráfico
- Captura de tráfico
- Análisis



UNIVERSID
POLITÉCNI
DE SAN LUIS PO

Riesgos

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Mi caso

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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

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”

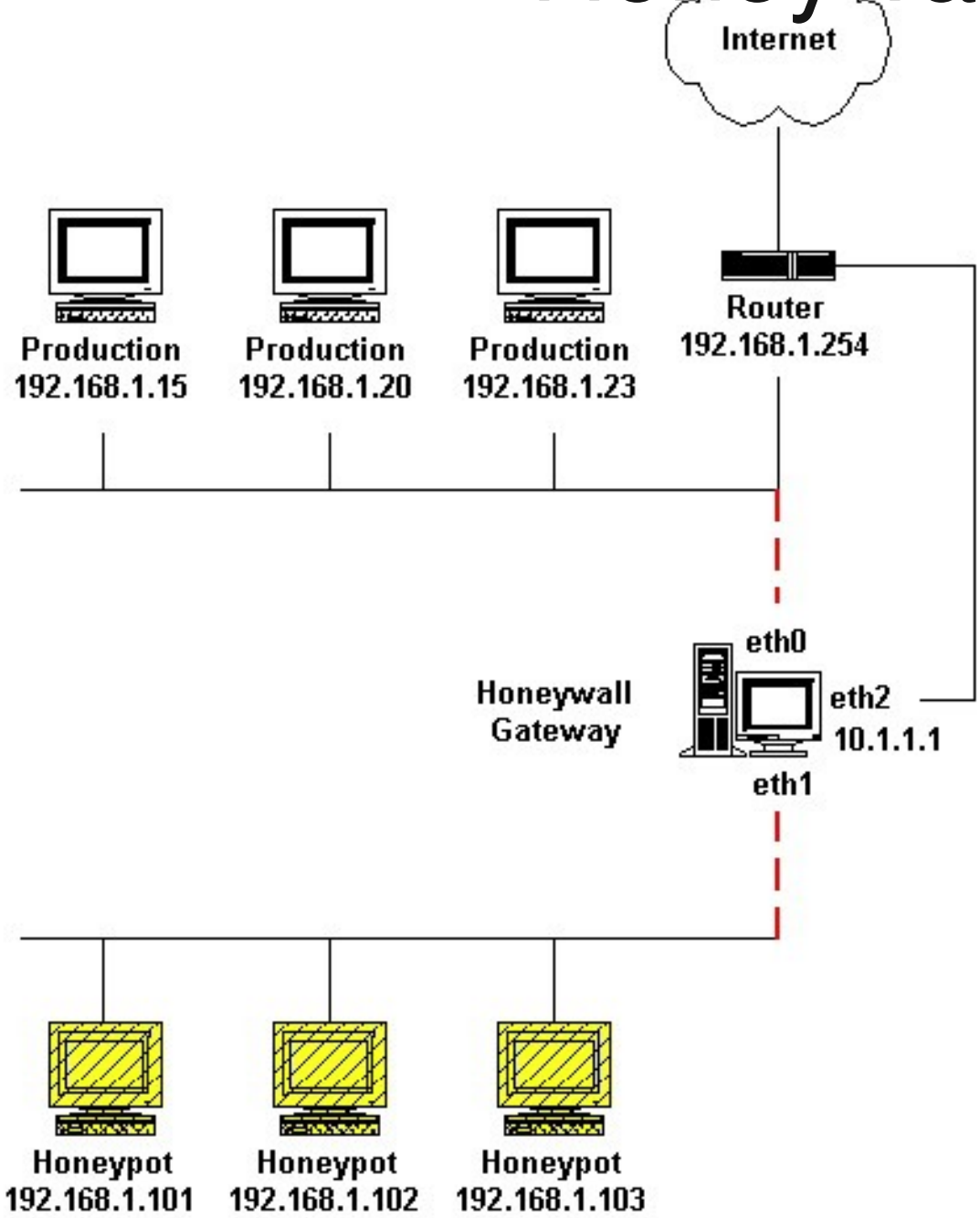
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Eligiendo la virtualización, o no

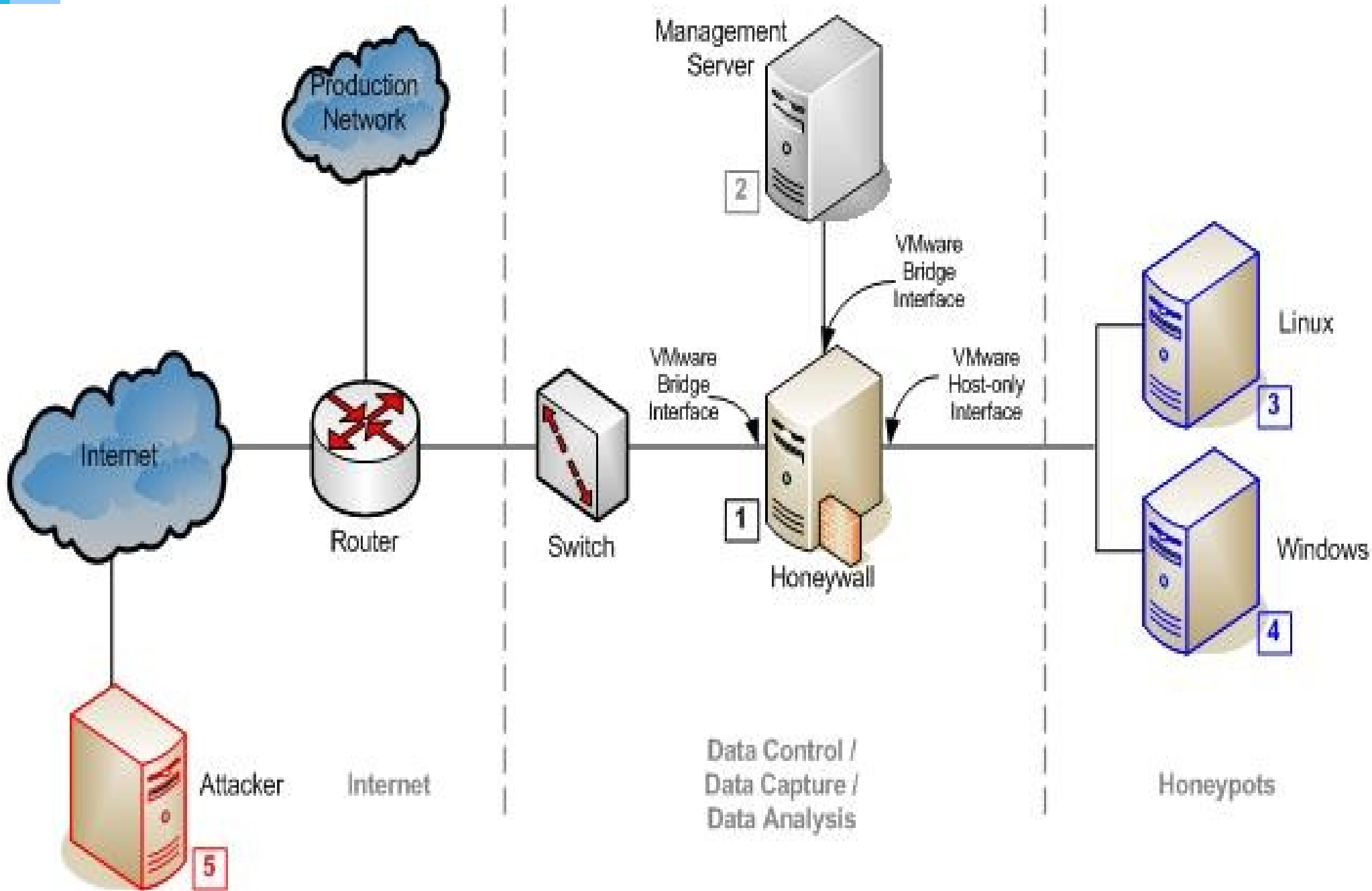
- Virtualización ?????
- qemu (Excelente opción)
- VMWare ????
- UML
- Virtuozo
- Xen

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Honeywall


Internet
Production
192.168.1.15
Production
192.168.1.20
Production
192.168.1.23
Router
192.168.1.254
eth0
Honeywall
Gateway
eth2
10.1.1.1
eth1
Honeypot
192.168.1.101
Honeypot
192.168.1.102
Honeypot
192.168.1.103

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.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Todo lo que hicimos en 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 swicthc virtuales

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Algunos datos del ITSLP

- Diversos intentos automáticos de explotación (a toda la red, no solo al honeynet)
- Hasta el día 25 de Septiembre de 2006 no se ha comprometido ninguna máquina.

- Ataque del ircbot
- Ataque a Mambo y Joomla

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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 estadisticos inciales.
- 5. Ejecutar tcpdstat para obtener información estadística básica.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

- 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.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

- 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.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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.
- Unir esfuerzos con el MHP.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Trabajo a futuro

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Agradecimientos

- A la UPSLP :
  - Por el apoyo para el viaje
- MHP
- Organizadores de las Jornadas
  - Por la invitación
- La comunidad FOSS ...

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Referencias

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

¿ 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
hugo@honeynet.org.mx

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ