

# Honeynets, conoce a tu enemigo

§ Raúl Siles



V Foro de seguridad RedIRIS  
Detección de Intrusiones  
12 y 13 de Abril de 2007

# Ponente

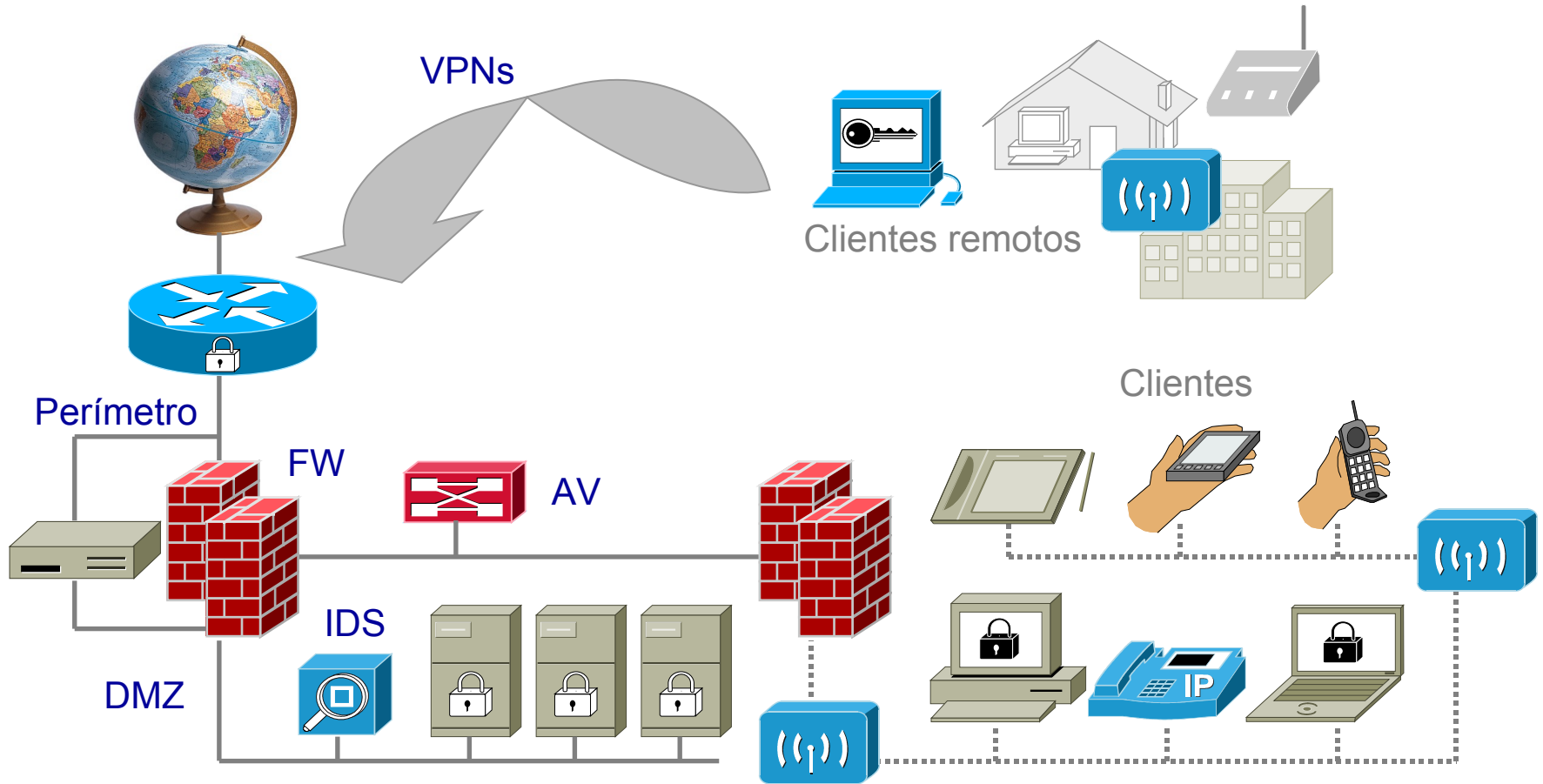
- Raúl Siles
- GSE
- Consultor Independiente de Seguridad
- Miembro del Spanish HoneyNet Project

[www.raulsiles.com](http://www.raulsiles.com)

# Índice

- Detección y respuesta ante incidentes en la actualidad
- Logs, logs y más logs
- Sun Tzu
- Honeynets, conoce a tu enemigo
- Demostraciones prácticas:
  - Walleye & Sebek

# Detección y respuesta ante incidentes 2007



# Un ejemplo de incidente...

- Llamada a las 20:30 un martes
- Cliente multinacional con múltiples sedes en España
- Varios ficheros críticos borrados en un entorno Unix
- Ocurrió a primera hora de la mañana (¡hace 12 horas!)
- Impacto crítico en el negocio
- ¿Qué podemos hacer?

# ... resolución del incidente



# ¿Qué es necesario para investigar los incidentes?



# Logs, logs y más logs

- *Firewalls* & Concentradores VPN & *Proxies*
- IDS/IPS: red, sistemas & herramientas de integridad de ficheros
- Sistemas: servidores, clientes, portátiles, PDAs...
- Dispositivos de red: *routers*, *switches*, puntos acceso, AAA...
- AV/*AntiSpyware*: cliente & servidor
- *Wireless* IDS, bluetooth, móviles, blackberries...
- Infraestructura PBX & VoIP
- Aplicaciones: Web, CRM, ERP, propias...
- Bases de datos
- ...

Correlación: Syslog o SIM o SEM o ...



# Resumen

Complejidad SIC

Avances en los ataques

Detección y respuesta ante incidentes

Honeynets

# Sun Tzu

- Vivió en el 544-496 AC
- China
- General militar, mercenario, aristócrata
- “Maestro del sol”

- Libro: “The Art of War”

<http://www.gutenberg.org/etext/132>

(Traducción de 1910, Lionel Giles)



# Sun Tzu - "The Art of War"

"If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle."

# Honeynets

字印 び 技す 国出のシ品 致 最 二 関 には 証 密 万

TRIXIT IS ALLAROUND US ITISTHERE WHEN YOU WA  
THE MATRIX HEIS THE ONE DREAMWORLD NEO

及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一

字 印 び 技 す 国 出 の シ 品 致 最

ALLAROUND US ITISTHERE WHEN YOU WATCH TELEVISION  
TISTHERE WHEN YOU WATCH TELEVISION

術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ

IX HEIS THE ONE DREAMWORLD NEO ANAGENT TRINIT  
に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一 二 関 には 証 密 万

国 出 の シ 品 致 最 一 二 関 には 証 密 万

EAMWORLD NEO ANAGENT TRINITTY WHAT IS YHE MAT  
US ITISTHERE WHEN YOU WATCH TELEVISION

の 精 及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ 品 致

給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国

に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一 二 関 には 証 密 万

の 文 精 刷 の 精 及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す

HEIS THE ONE DREAMWORLD NEO ANAGENT TRINITTY W  
HE MATRIX IS ALLAROUND US ITISTHERE WHEN YO  
EAMWORLD NEO ANAGENT TRINITTY WHAT IS YHE MAT

給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一

に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一 二 関 には 証 密 万

の 文 精 刷 の 精 及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す

給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一

に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一 二 関 には 証 密 万

の 文 精 刷 の 精 及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す

給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一

に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一 二 関 には 証 密 万

の 文 精 刷 の 精 及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す

給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一

に 美 と 字 印 び 技 す 国 出 の シ 品 致 最 一 二 関 には 証 密 万

の 文 精 刷 の 精 及 術 文 写 て 感 ぜ 給 し 会 親 美 イ 力 版 も し 保 の 文 精 な フ ト 社 明 を に 美 と 字 印 び 技 す 国 出

MATRIX

# ¿Porqué se llaman Honeynets?



# Honeynets: Principios

- Definición de Honeynets / Honey pots:  
*Recurso de seguridad cuyo valor se basa en el uso no autorizado o malicioso del mismo*
- Solución y tecnología de seguridad para la captura de información
- Detección, análisis y respuesta ante incidentes de seguridad
- Aprender las herramientas, tácticas y motivaciones de la comunidad *blackhat*
- Compartir las lecciones aprendidas

Mejorar la seguridad del entorno de IT

# Honeynets: Detalles

- Simular y/o replicar los entornos de producción
- Responder a las 5+1 W's de los incidentes de seguridad: *What, where, when, who, why + How*
- Niveles:
  - Control de datos (Data Control)
  - Captura de datos (Data Capture)
  - Análisis de datos (Data Analysis)
- Reducido valor directo en la protección de redes y sistemas



# Honeynets: Ventajas

- Cualquier tráfico es ilegítimo por naturaleza
- Detectar nuevos ataques (*0-day*)
- Notificación temprana de incidentes
- Reducir el número de falsos positivos
- Gestionar los innumerables *logs* recolectados (si tienes suerte... 😊)
- Entrenar al equipo de respuesta ante incidentes y análisis forense

# Honeynets: Leyes

- Aspectos legales:
  - Responsabilidades: daños colaterales
  - Monitorización de datos: cabeceras frente a contenido
  - Evidencias forenses
- ¿Realidad?

# Honeynets: Tipos

- Nivel de interacción: alto o bajo
- La mejor opción depende de los objetivos de la Honeynet
- Alto: aplicaciones o sistemas reales (o virtuales)
- Bajo: software de emulación
  - Nepenthes, Honeyd, Honeytrap

# The HoneyNet Project

*“Promote honeynet technologies to improve Internet security”*

- Lance Spitzner, 1999
- Enseñar, informar, investigar:  
*Security challenges, tools, papers...*
- The HoneyNet Research Alliance

**The HoneyNet**  
P R O J E C T

<http://www.honeynet.org>

# Spanish HoneyNet Project

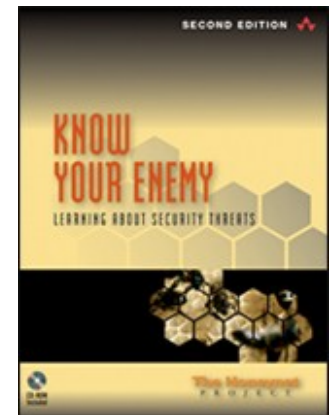
- Fundado en el verano de 2004
- Objetivos
- SotM 32 - RaDa
- Número de miembros actual: 4
- Honeynets: W2K3, SPAM, WiFi...



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

# Conoce a tu enemigo

- ¿Cómo podemos defendernos del enemigo, cuando ni siquiera sabemos quién es?
- KYE: Know Your Enemy
- Objetivo: “Compartir las lecciones aprendidas”
- *Whitepapers*: KYE & individual
- KYE Book, 2nd Ed



<http://www.honeynet.org/papers/index.html>

# Evolución de los ataques: pasado

- Comunicaciones mediante túneles IPv6 (2002)
- Extorsión en Internet mediante DDoS (2003)
- Fraude automático de tarjetas de crédito (2003)
- Honeynets en universidades (2004)
- Botnets: SPAM, DoS (2005)
- Phising (2005)

# Evolución de los ataques: futuro

- Ataques en aplicaciones Web (2007)
  - GHH - The "Google Hack" Honeytrap
- Ataques en clientes (durante 2007)
- Ataques a sistemas *SCADA*
- Procesado de ataques dinámico:
  - Conexiones a puertos arbitrarios y emulación y análisis de *shellcode*
- Global Distributed Honeytrap (GDH)
- Otros... 😊



# Honeynets servidor y cliente

- Honeynets servidor: esperar a recibir los ataques
- Honeynets cliente: ir en busca de ser atacado, simulando las acciones de los usuarios
  - Capture-HPC (alta interacción, VM & IE)
  - HoneyC (baja interacción, firmas)
  - MS HoneyMonkeys
  - McAfee SiteAdvisor (IE and Firefox)
  - Honeyclient

# Generaciones de Honeynets

- Gen I – Arquitectura con *Data Control y Data Capture*
- Gen II – Mejoras:
  - *Bridge* a nivel 2, filtrado, sistema de alertas, *Sebek v2.x*, basado en CD-ROM
- Gen III – *Data Analysis*

GenI (1999) – GenII (2002) – GenIII (2005) – *Kanga* 2007

# Honeywall CD-ROM

- Punto de entrada/salida a la Honeynet (*gateway*)
- Solución todo en uno
- Fácil de implantar y gestionar
- Basado en un único CD-ROM
- Versiones: Eeyore y Roo



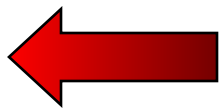
Eeyore (Mayo 2003) – Roo (Mayo 2005) – Roo 1.2 (2007)

<http://www.honeynet.org/tools/cdrom/>

# Subsistemas del Honeywall

## Data Control

Iptables  
Rate-limitting  
Snort-inline



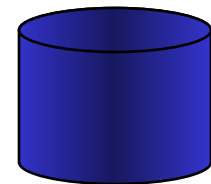
## Data Capture

Iptables logs  
Snort alerts  
p0f  
Hpots Sebek  
Tcpdump

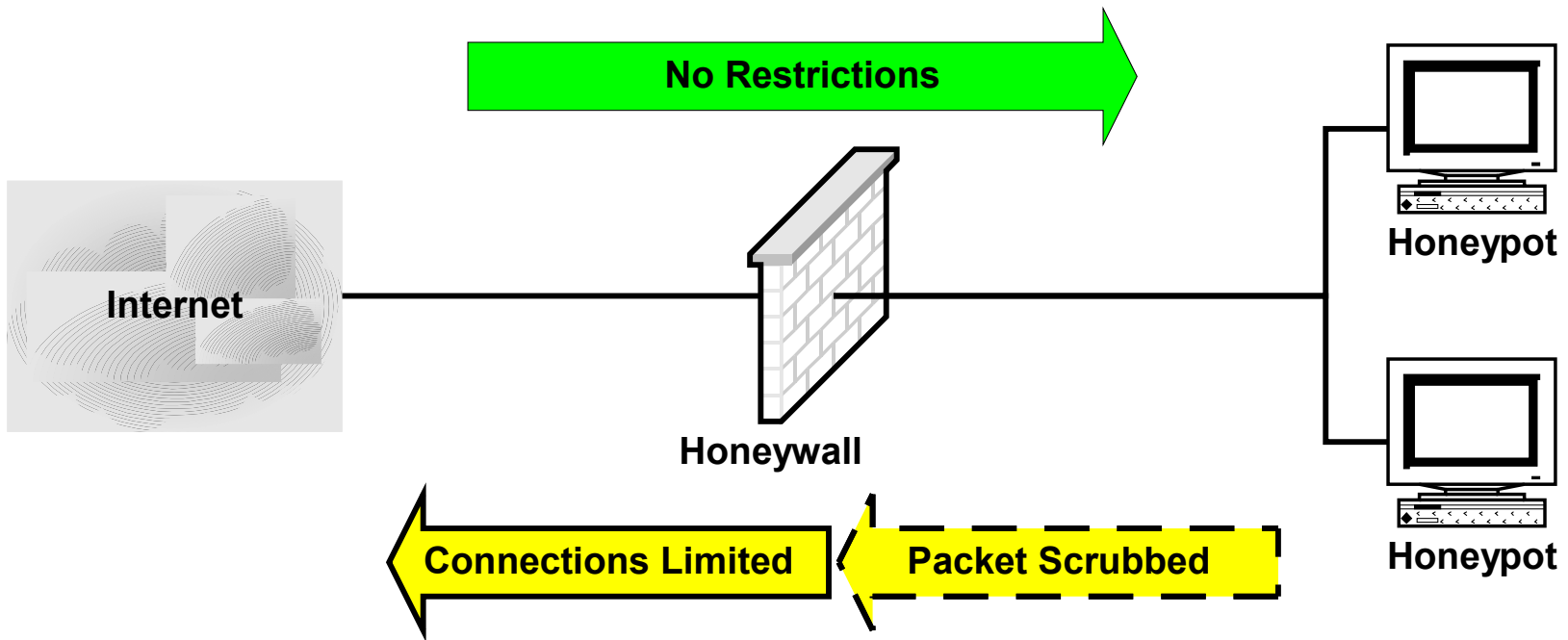


## Data Analysis

MySQL  
Argus + Hflow  
Swatch (alerts)  
Walleye



# Data Control



# Data Capture

- Logs del firewall (iptables)
- Alertas del IDS (Snort)
- Identificación pasiva de SO (p0f)
- Captura avanzada de datos (Sebek)
- Tráfico de red (tcpdump)
- Alertas del IPS (Snort-inline)

# Data Analysis

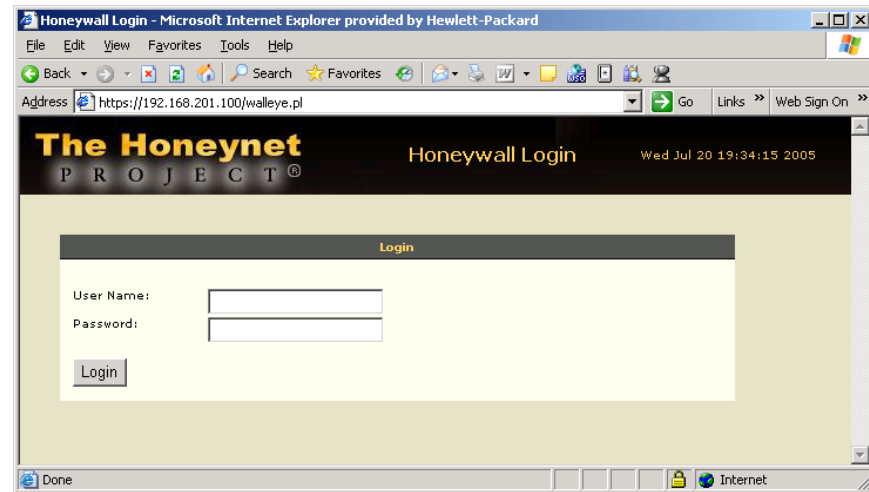
- Correlación de información en una base de datos MySQL
- Información de flujos de tráfico y relaciones (Argus + Hflow)
- Logs del firewall & alertas del IDS (Swatch)
- Interfaz gráfico Web (Walleye)

# El problema del análisis de datos

- Lecciones aprendidas:

“... necesidad de disponer de una herramienta de análisis de datos potente y fácil de usar.”

- Solución: Walleye



[https://IP\\_HoneyWall/walleye.pl](https://IP_HoneyWall/walleye.pl)



# Capacidades de Walleye

- Administración del sistema:
  - Estado del sistema y administración del SO
  - Administración y configuración del Honeywall
  - Gestión de usuarios y reglas de Snort
- Análisis de datos:



# Walleye: múltiples vistas

- Estadísticas de tráfico
- Detalles de flujos de tráfico
- Alertas del IDS
- Información avanzada de las actividades en el sistema
  - Procesos en ejecución
  - Actividades detalladas de cada proceso

# Walleye: análisis de datos

The screenshot shows the 'Connections related to 192.168.100.66 After Mon Nov 28 00:00:00 2005 Before Mon Nov 28 23:59:59 2005' section. It includes a calendar for November 2005 and a table of connections:

Start	End	Protocol	Source	Destination	Details
November 28th 03:44:28 00:00:03	192.168.100.66	<->	192.168.100.150		ICMP 0 0 kb 4 pkts ->
November 28th 03:44:51 00:00:00	192.168.100.66		192.168.100.66		UDP netbios-ns 0 kb 0 pkts ->
November 28th 03:44:51 00:00:01	192.168.100.150		192.168.100.150		<-1-NETBIOS SMB transOpen buffer overflow attempt
November 28th 03:44:51 00:00:01	192.168.100.150		192.168.100.150		<-3-SHELLCODE x86 NOOP
November 28th 03:44:51 00:00:01	192.168.100.150		192.168.100.150		<-3-SHELLCODE x86 NOOP

The screenshot shows the 'Flows' section with a table of total flows and a bar chart of KBytes Transferred over time.

Out	In	Out
0	3,339	262
0	77,817	13,002

The bar chart shows KBytes Transferred (yellow bars) and N/10 Alerts (red bars) from 10:00 to 10:00. The search interface below has the following fields:

- Start: Nov 15 2005 10:11:48
- End: Nov 16 2005 10:11:48
- Prefix: ANY
- Port: 0
- Pcap File: [Dropdown]

The screenshot shows the 'Process Summary' for the 'smbd' process on host 192.168.100.150, PID 2340. It includes a 'Process Tree' diagram showing the following structure:

```
graph TD; A[Host: 192.168.100.150, PID: 2340, smbd] --> B[Host: 192.168.100.150, PID: 2341, sh]; A --> C[Host: 192.168.100.150, PID: 2342, sh]; B --> D[Host: 192.168.100.150, PID: 2344, id]; B --> E[Host: 192.168.100.150, PID: 2345, unime]; C --> F[Host: 192.168.100.150, PID: 2347, cat]; C --> G[Host: 192.168.100.150, PID: 2348, cat];
```

# El problema de la captura de datos

¿Cómo capturar las actividades de los atacantes sin que lo sepan?

- Captura del tráfico de red:  
*Ethereal – “Follow TCP Stream”*
- ¿Cómo superar el uso de cifrado?  
(SSH, SSL, IPSec...)
- No es posible sino se tiene la clave hasta que apareció...

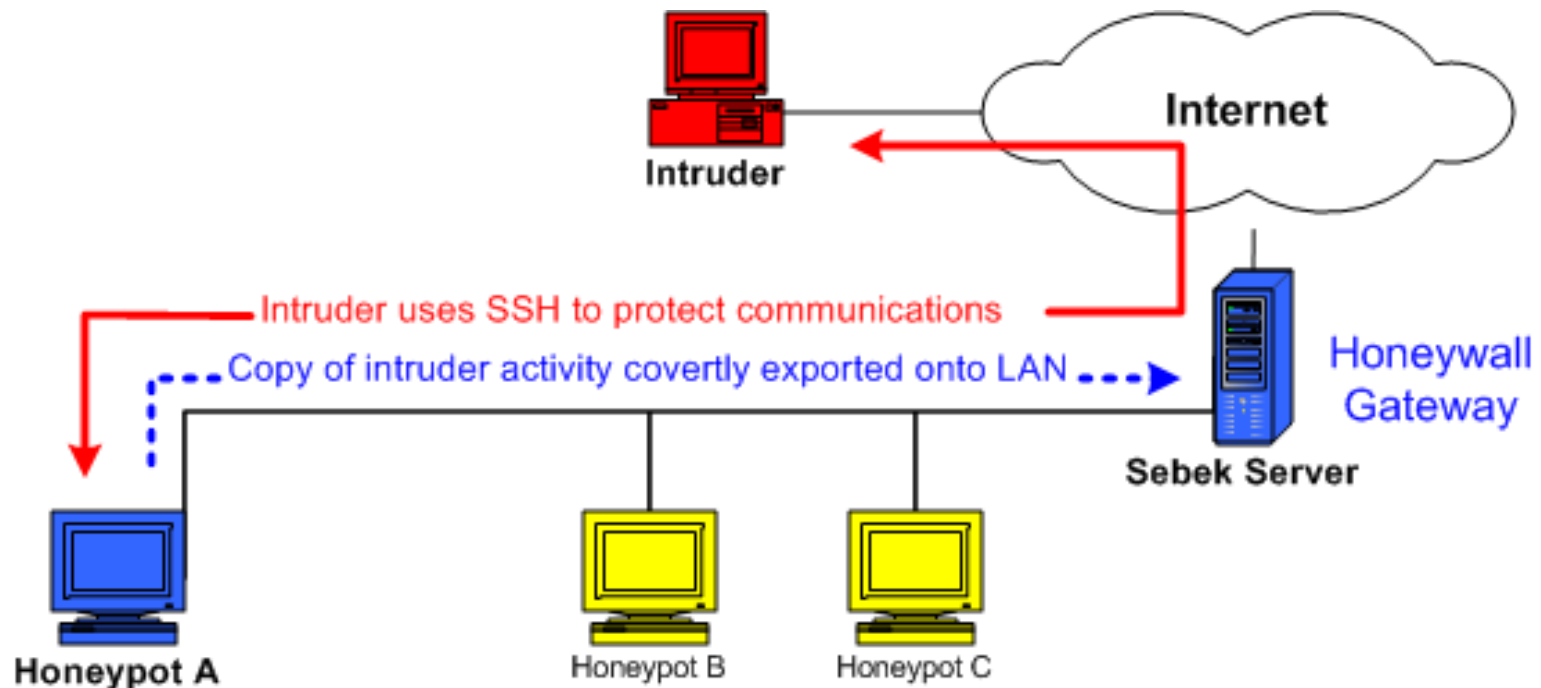
# Sebek

- Herramienta de captura de datos
- Permite visualizar incluso tráfico cifrado sin disponer de la clave
- Monitorización de teclas pulsadas
- Similar a un rootkit de kernel:
  - LKM – Linux, Solaris, \*BSD...
  - Driver de Kernel - Windows

<http://www.honeynet.org/tools/sebek/>

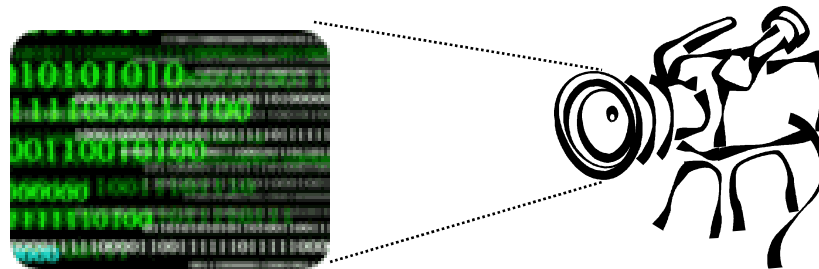


# Sistema de comunicación de Sebek



# Parche “write” para Sebek

- Sebek permite capturar los datos tecleados por el atacante, pero ...
- El parche permite capturar también la respuesta recibida por el atacante (llamada al sistema “write”)



# Monitorización con Sebek “write”

```
SSP-Honeywall - VMware Workstation
File Edit View VM Team Windows Help
RH9 SSP-Honeywall RH9 WinXP
[root@ssphoneywall ~]# sbk_extract -i eth1 -p 29905 2>>/dev/null; ./sbk_viewer.pl
scsictrl.o installed successfully
[root@localhost sebek-linux-3.0.3-write]#
#uname -a
Linux localhost.localdomain 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686 i686 i
386 GNU/Linux
[root@localhost sebek-linux-3.0.3-write]#
#id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
[root@localhost sebek-linux-3.0.3-write]#
#ls
acconfig.h          config.log          install-sh          scsictrl.o
aclocal.m4          config.status      Makefile           scsi_.o
af_packet.diff     config.sub         Makefile.am       sebek.c
AUTHORS            configure         Makefile.in       sebek.c.old
ChangeLog          configure.in      missing           sebek.h
cleaner.c          COPYING          mkinstalldirs    sebek.h.old
cleaner.o          depcomp          NEWS              sebek-linux-3.0.3-bin.tar
config.guess       fudge.h          parameters.sh     sebek.o
config.h           gen_fudge.pl     README            stamp-h1
config.h.in       INSTALL          sbk_install.sh
[root@ssphoneywall ~]# _
```

Comandos del atacante

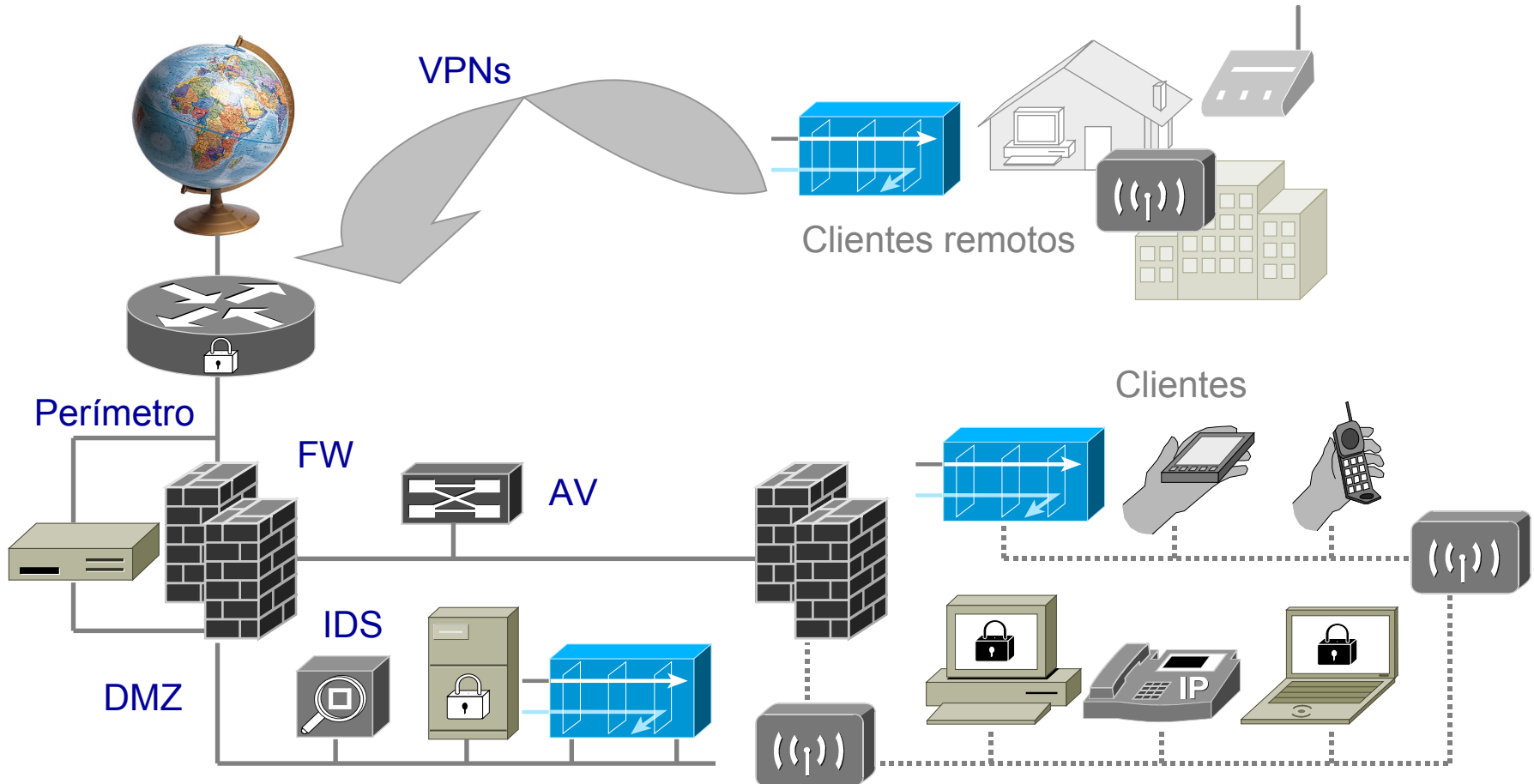
Respuesta recibida



# Siguientes pasos y usos...

- Análisis forense de sistemas
- Análisis forense de tráfico de red
- Recolección y análisis de *malware*
- Probar el plan de respuesta ante incidentes (CERTs)
- Sistemas de notificación de alertas tempranas
- Firmas de AV, SPAM, RBL...

# Despliegue de Honeynets



# Honeytérminos

- Honeypot
- Honeynet
- Honeywall
- Honeyclient (Honeymonkey)
- Honeystick
- Honeytoken





# Formación en Honeynets

- SANS Institute
- Security 554: Honeynets
- Curso de 1 día (2007)
- Sesiones pasadas en España, Londres y USA en 2006



<http://www.sans.org/staysharp/description.php?tid=354>

# ¡Muchas gracias!

- The Honeyney Project

<http://www.honeynet.org>



- Spanish Honeyney Project

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



- Raul Siles

<http://www.raulsiles.com>

