Honeynets, conoce a tu enemigo

Raúl Siles

V Foro de seguridad RedIRIS

Detección de Intrusiones

12 y 13 de Abril de 2007

Ponente

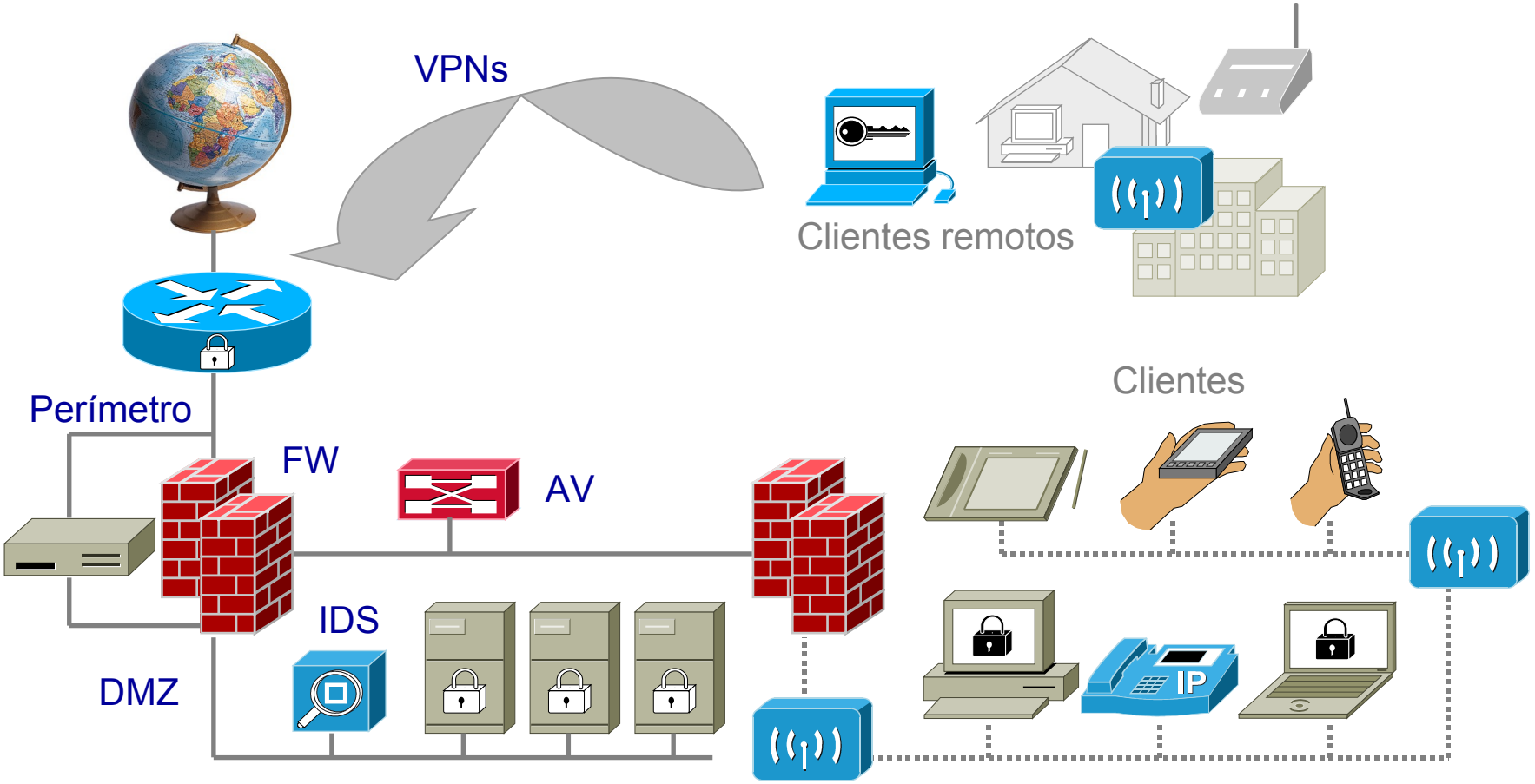
- Raúl Siles
- GSE
- Consultor Independiente de Seguridad
- Miembro del Spanish Honeynet Project

www.raulsiles.com

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

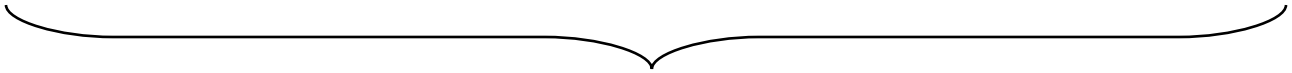
- *Firewalls* & Concentradores VPN & *Proxies*
- IDS/IPS: red, sistemas & herramientas de integridad de ficheros
- Sistemas: servidores, clientes, portátiles, PDAs…
- Dispositivos de red: *routers*, *switches*, puntos acceso, AAA…
- AV/*AntiSpyware*: cliente & servidor
- *Wireless* IDS, bluetooth, móviles,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

Correlación: Syslog o SIM o SEM o …

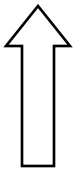
Resumen

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

¿Porqué se llaman Honeynets?

Atacante

€, $…

Víctima

Phising

Botnets

DDoS

SPAM

…

Honeynets: Principios

- Definición de Honeynets / Honeypots:
  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: W*hat, 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 PROJECT

http://www.honeynet.org

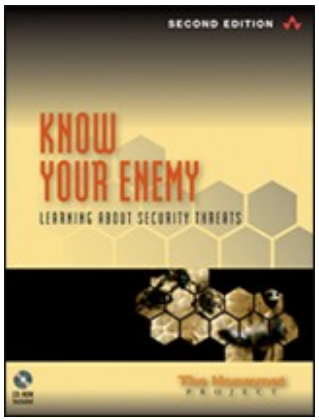
Spanish Honeynet Project

- 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" Honeypot
- 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 Honeynet (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

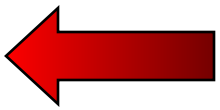
- Punto de entrada/salida a la Honeynet (*gateway*)
- Solución todo en uno
- Fácil de implantar y gestionar
- Basado en un único CD-ROM
- Versiones: Eeyore y Roo

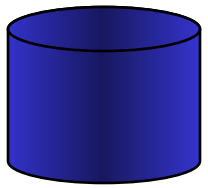
Eeyore (Mayo 2003) – Roo (Mayo 2005) – Roo 1.2 (2007)

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

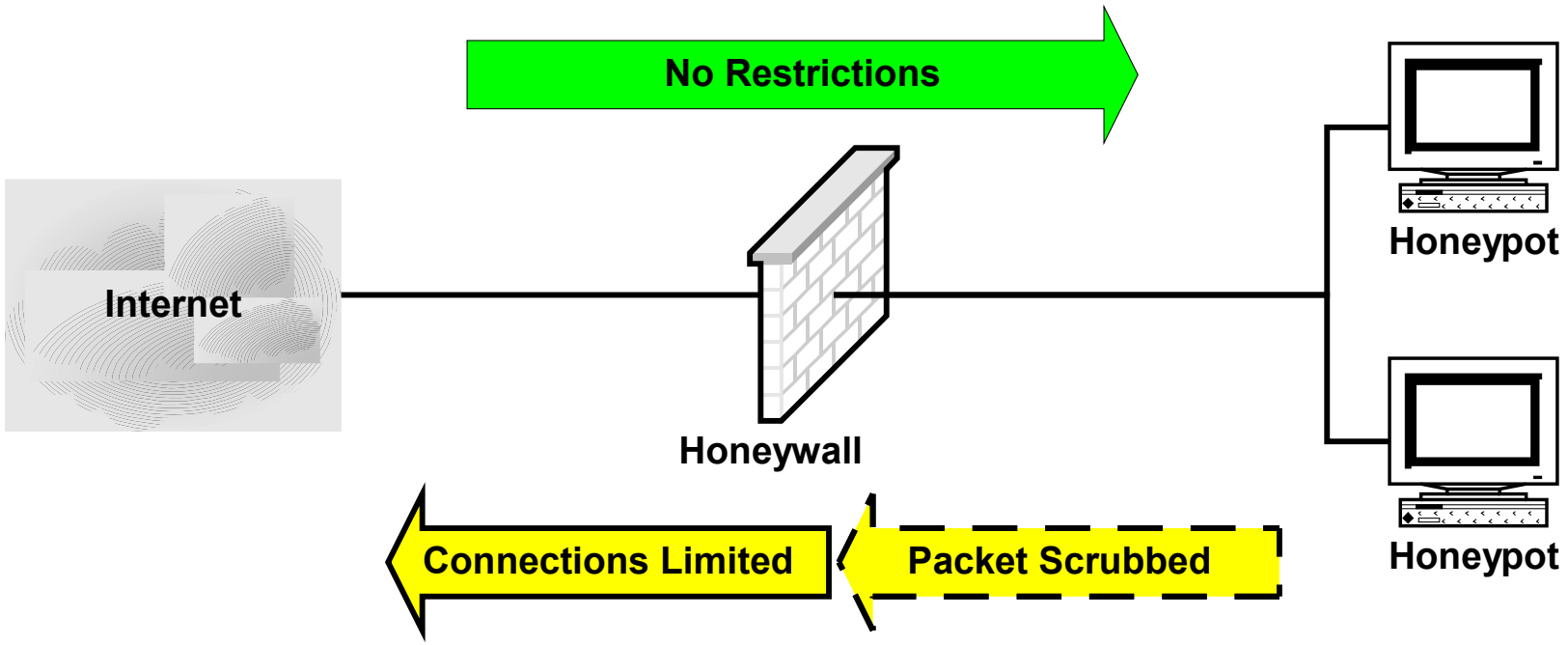
Subsistemas del Honeywall

Data Control	Data Capture	Data Analysis
Iptables	Iptables logs	MySQL
Rate-limitting	Snort alerts	Argus + Hflow
Snort-inline	p0f	Swatch (alerts)
	Hpots Sebek	Walleye
	Tcpdump	





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

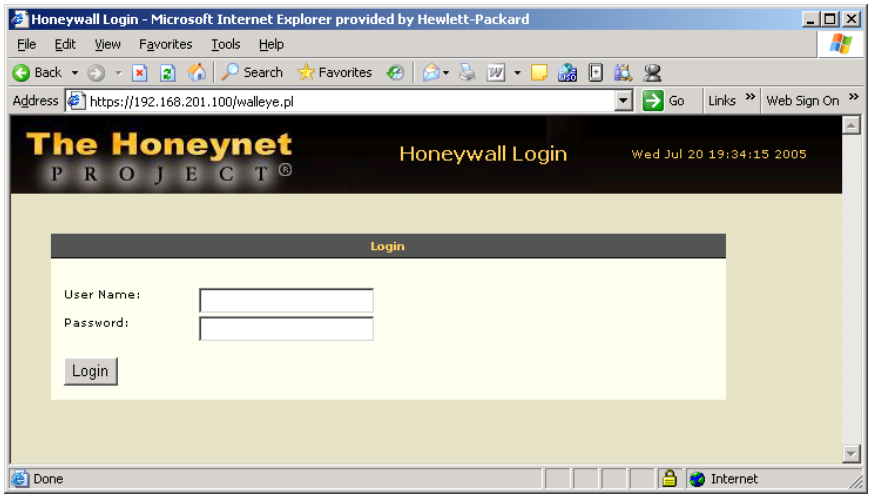
- Correlación de información en una base de datos MySQL
- Información de flujos de tráfico y relaciones (Argus + Hflow)
- Logs del firewall & alertas del IDS (Swatch)
- Interfaz gráfico Web (Walleye)

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

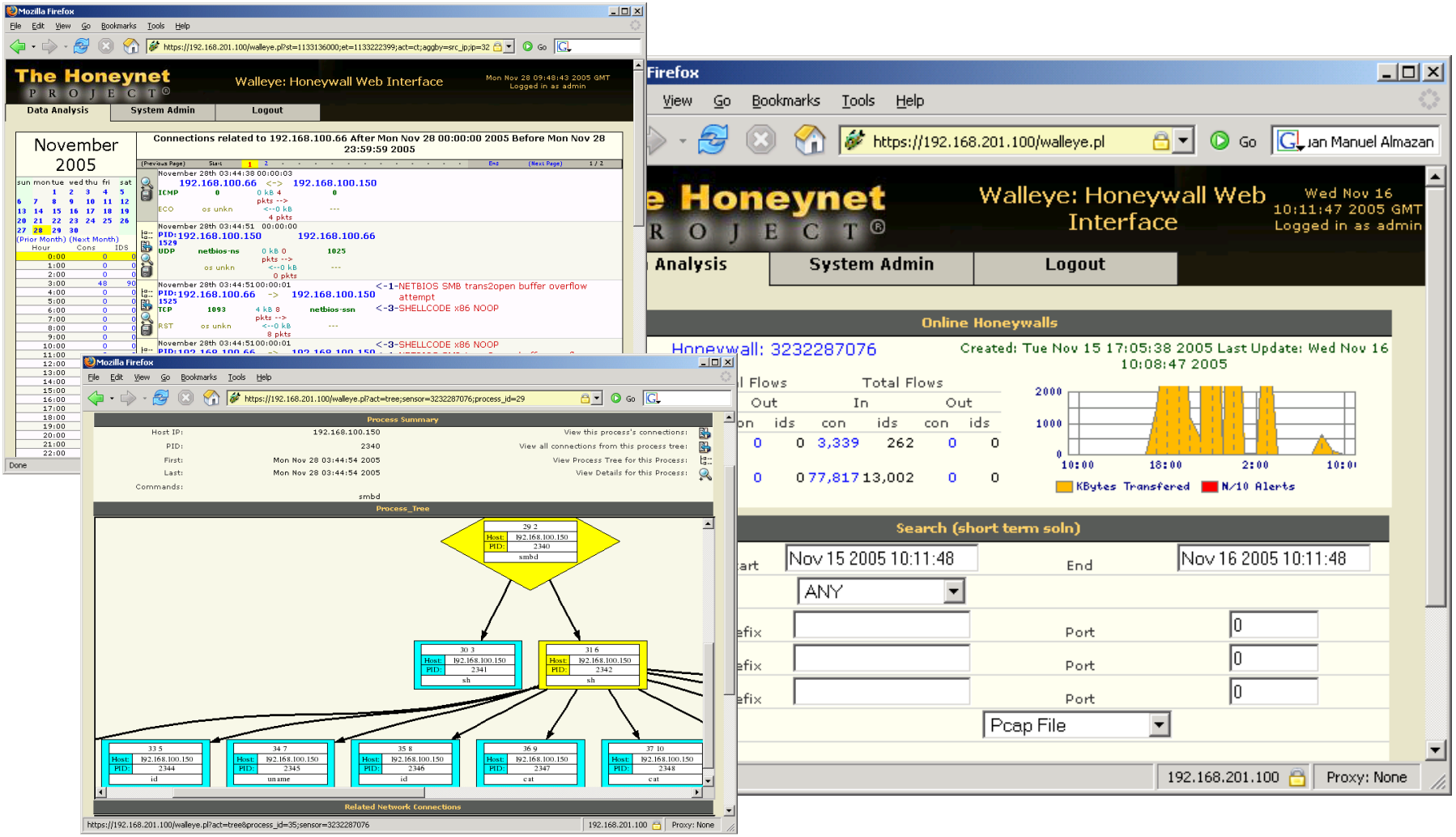
Capacidades de Walleye

- 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



El problema de la captura de datos

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

- Captura del tráfico de red:

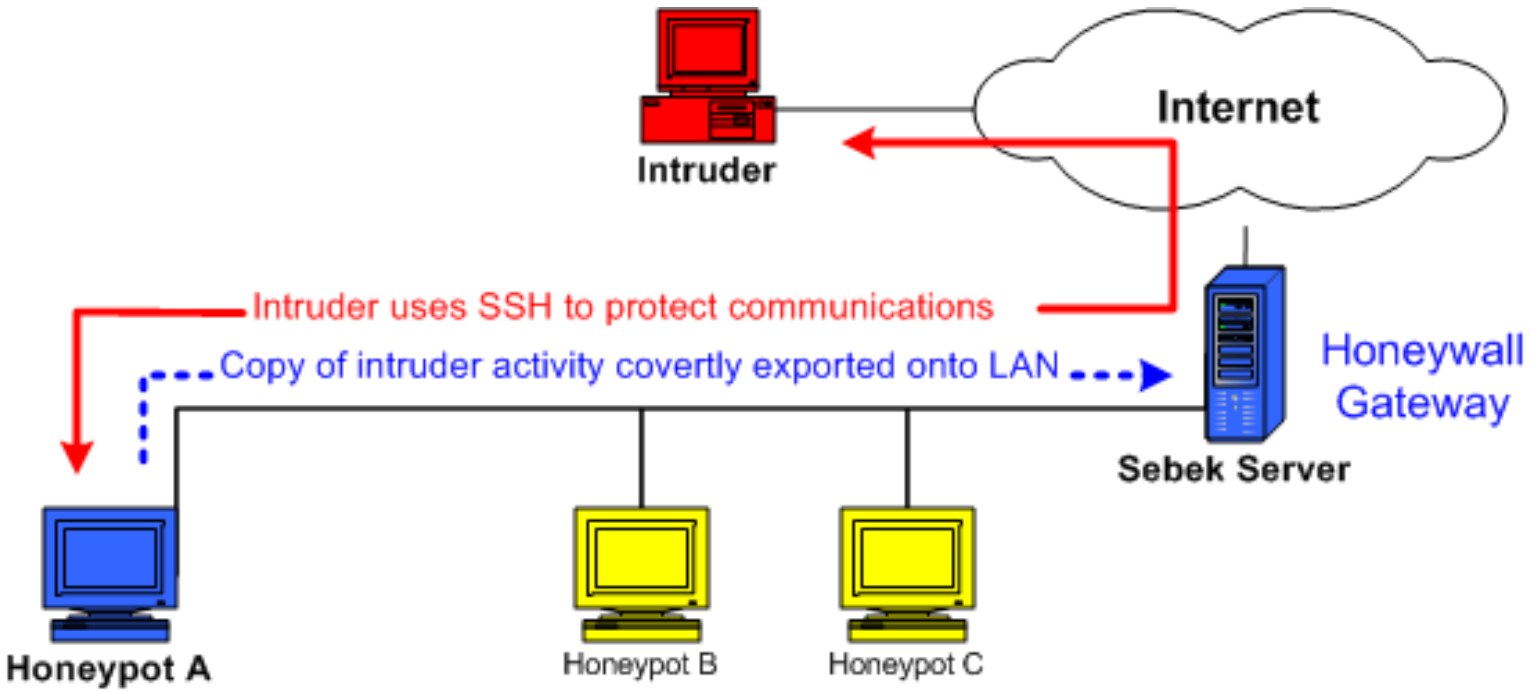
  Ethereal – "Follow TCP Stream"
- ¿Cómo superar el uso de cifrado? (SSH, SSL, IPSec…)
- No es posible sino se tiene la clave hasta que apareció…

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

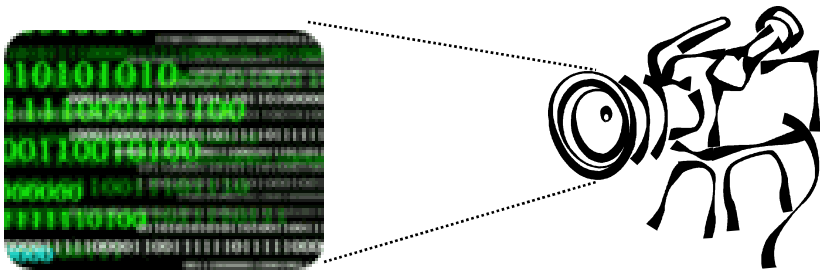
http://www.honeynet.org/tools/sebek/

Sistema de comunicación de Sebek



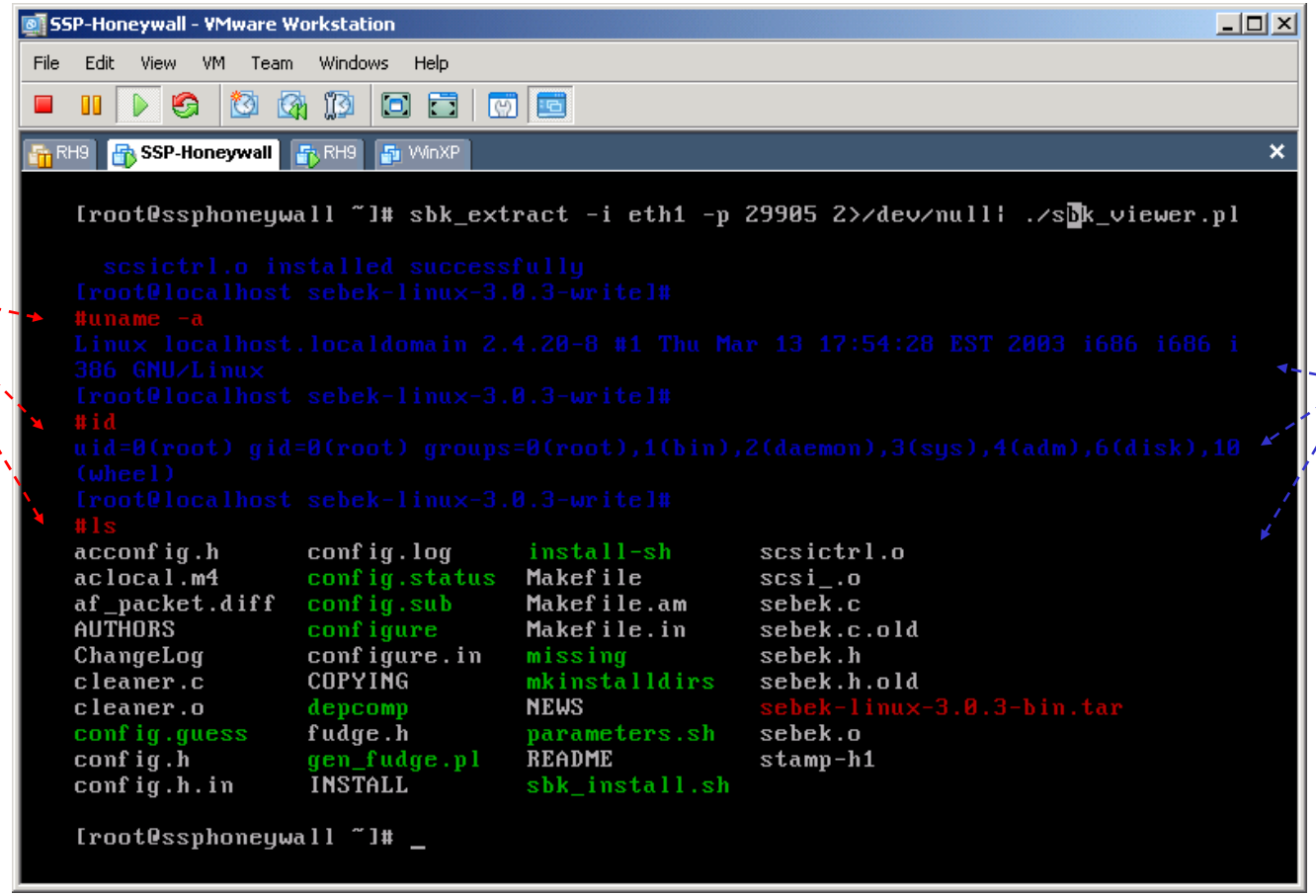
Parche “write” para Sebek

- 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”

Comandos del atacante

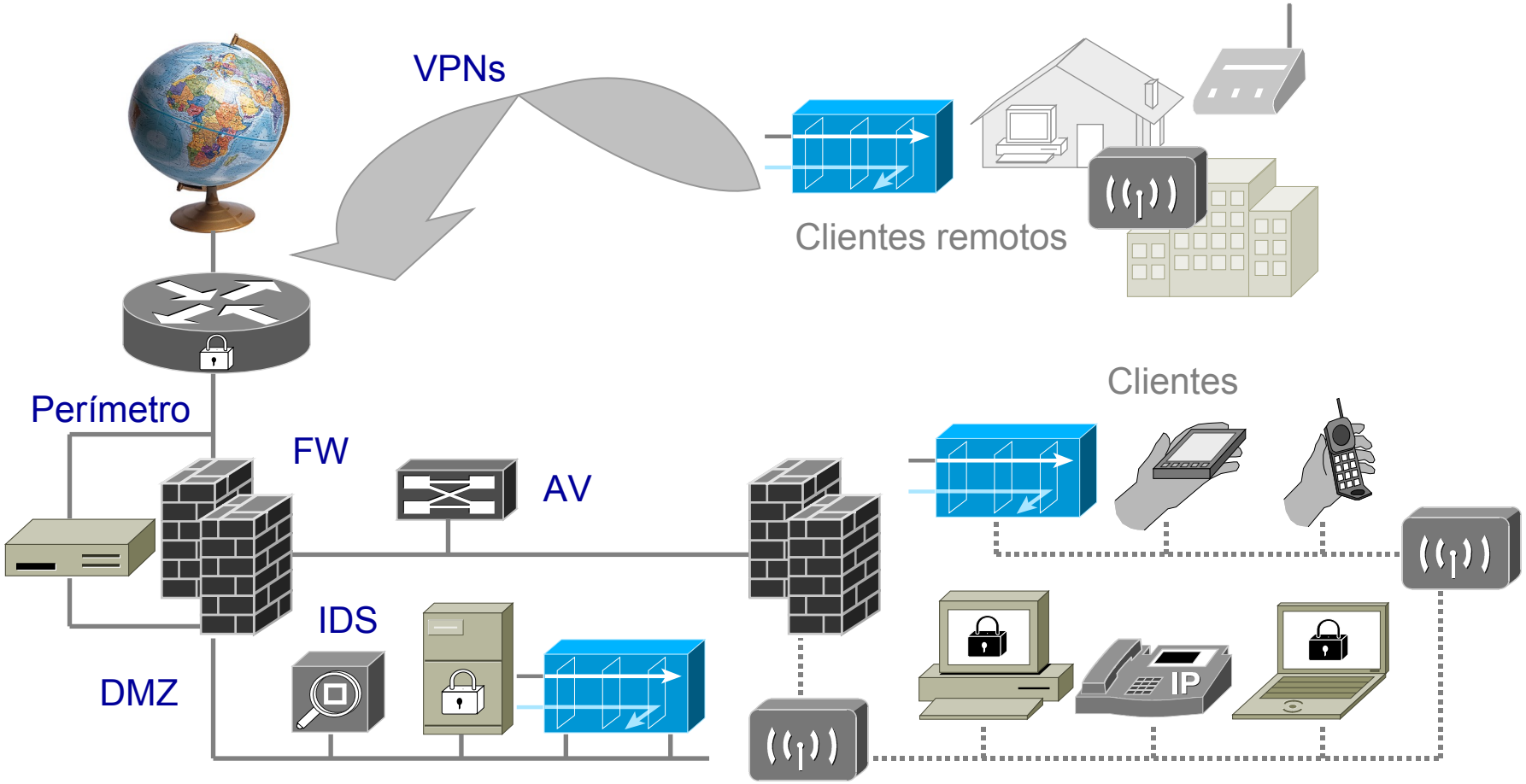


Respuesta recibida

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…

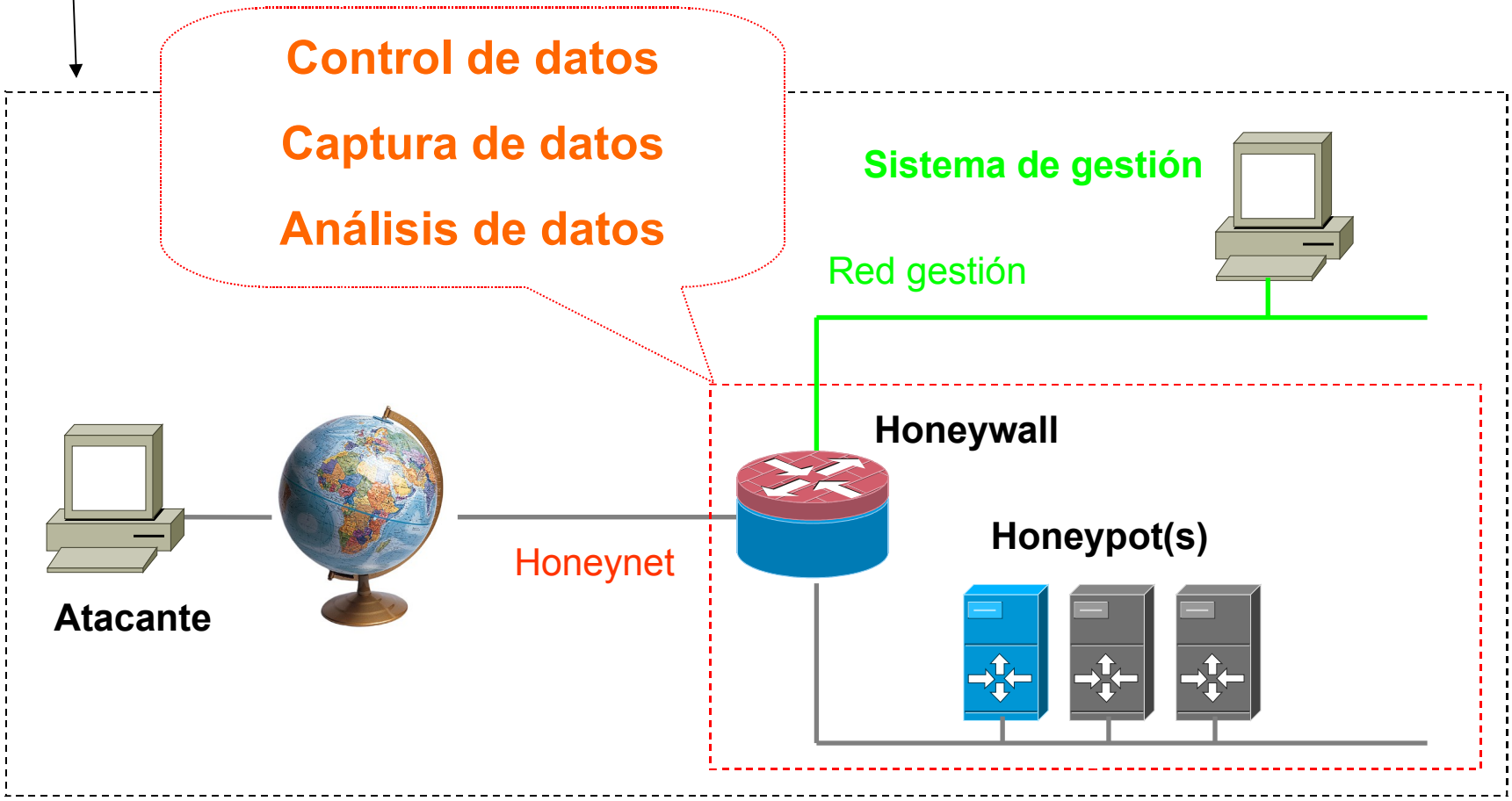
Despliegue de Honeynets



Honeytérminos

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

Demostraciones prácticas



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