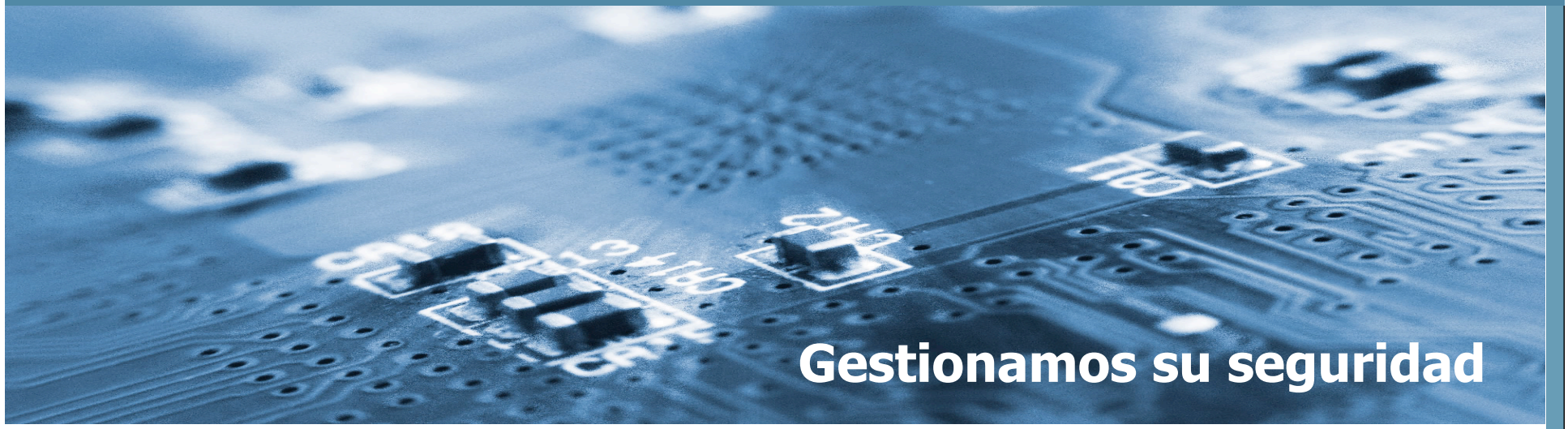
InetSecur S.L.



Análisis Forense

NCN 2K4 – 9-12 septiembre, 2004

INETSECUR

Índice

- Respuesta a incidentes
- Análisis forense
- Adquisición de Datos
- Herramientas
- Caso práctico

INETSECUR

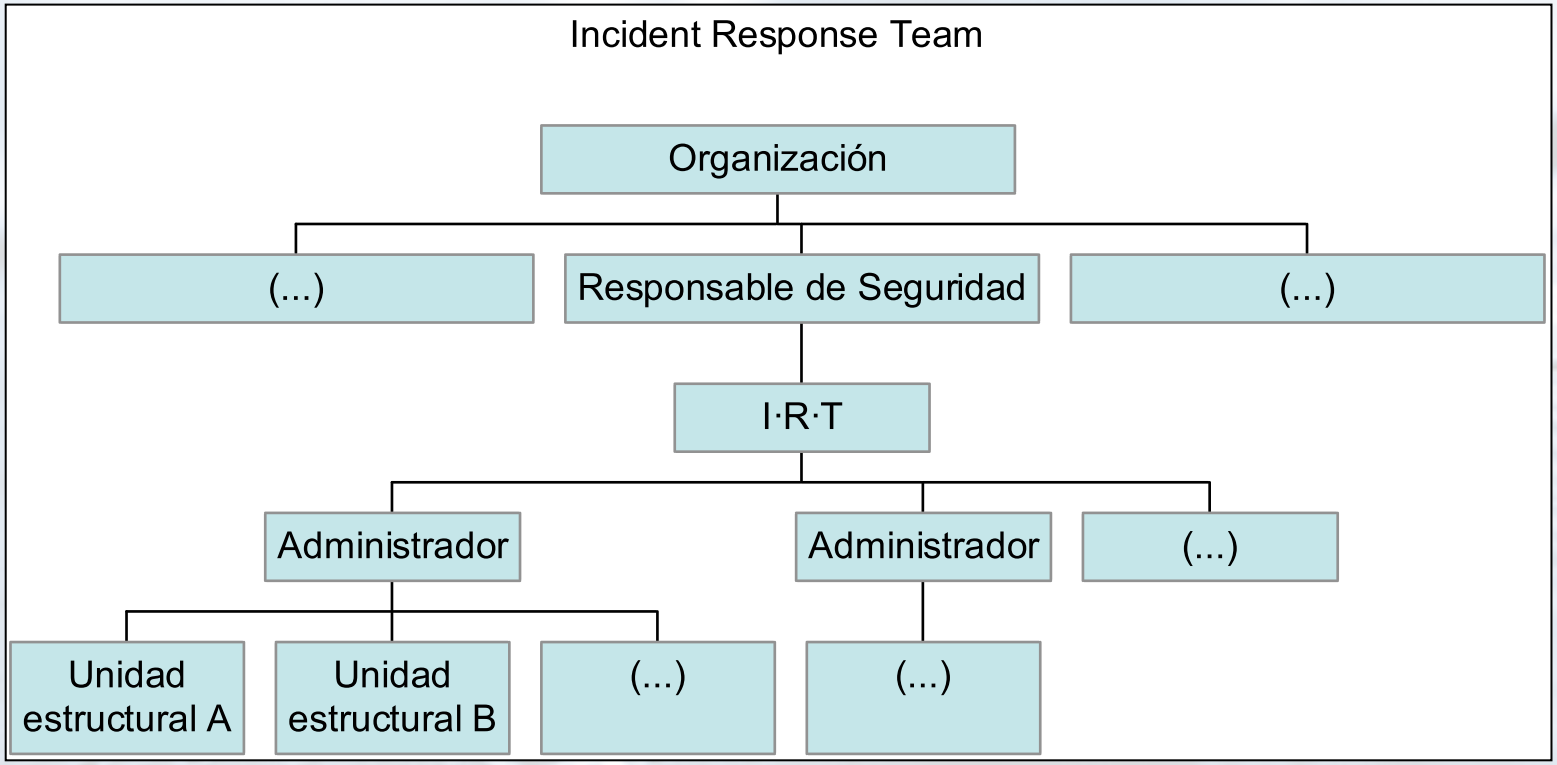
Respuesta a Incidentes

- Administración centralizada de los incidentes de seguridad (internos y externos)
  - Permite gestionar la seguridad informática de la organización desde una perspectiva global.
- Cuando (no si) suframos un incidente, querremos:
  - Alerta temprana.
  - Máxima información.
  - Mínimo coste (en tiempo, dinero, recursos en general).
  - Sin perder tiempo de servicio.

INETSECUR

Respuesta a Incidentes

- IRT: Equipo de Respuesta a Incidentes



INETSECUR

Análisis Forense

- Motivación: Obtener información acerca del incidente
  - Procedencia
  - Punto de entrada
  - Herramientas
  - Alcance
  - Consecuencias
- Ayuda a la toma de decisiones en el marco de la respuesta a incidentes.

INETSECUR

Análisis Forense

- Evidencia Digital
  - ¿Qué es Evidencia Digital?
    - Una línea de texto en un log.
    - La hora de último acceso de un fichero.
    - Una cookie en un disco duro.
    - Una MAC en una tabla ARP.
    - El uptime de un sistema.
    - Un fichero en disco.
    - Un proceso en ejecución.
    - ...
  - ¿Dónde la encontramos?
    - PCs (HD, RAM).
    - PDAs, teléfonos, cámaras digitales...
    - Routers, switches...
  - Cualquier dato en la memoria volátil o fija de un dispositivo puede ser Evidencia Digital.

INETSECUR

Análisis Forense

- Metodología
  1. Estudio preliminar
     - Descripción del caso: qué ha ocurrido, a dónde se desea llegar.
     - Recogida de información sobre las organizaciones, redes, etc. implicadas.
     - Identificación de los elementos relevantes: escenario, sistemas, agentes.
  2. Adquisición de datos
     - Copia de las fuentes de información relevantes.
     - Aplicación de mecanismos necesarios para preservación de la evidencia: hashes, timestamping.
  3. Análisis
     - Se plantean teorías sobre lo sucedido. Según la evidencia encontrada, estas teorías se refuerzan o descartan.
  4. Presentación
     - Exposición y defensa, ante un cliente o en un tribunal, de la validez de los resultados obtenidos.

Análisis Forense

- Consideraciones
  - Todo el proceso debe estar documentado.
    - Cualquier investigador, partiendo de los datos originales, y aplicando las herramientas y procedimientos que describamos, será capaz de llegar a los mismos resultados.
  - Debe, por supuesto, respetarse la legislación aplicable, así como las políticas de la Organización.

INETSECUR

Análisis Forense

- Aproximación tradicional
  - Fuentes de información:
    - Logs (del sistema comprometido y de otros).
    - Capturas de tráfico de red (completas, IDSs...).
    - Ficheros del sistema comprometido:
      - Ingeniería inversa
      - mac-times
  - Temporalización → Correlación

INETSECUR

Adquisición de Datos

- Copia de la información contenida en un sistema.
  - Toda la contenida en soportes no volátiles.
  - En algunos casos, también la contenida en soportes volátiles.

- El dilema: ¿apagamos el sistema, o antes interactuamos con él?
  - Si no lo apagamos, podremos ver las conexiones de red activas, los procesos en ejecución, los usuarios conectados...
  - Sin embargo, el sistema puede estar troyanizado y ocultar esa información. Además, se contamina la escena del crimen.

INETSECUR

Adquisición de Datos

- El proceso debe realizarse arrancando el sistema en un entorno limpio y controlado. Por ejemplo:
  - Se arranca el sistema comprometido utilizando un Live CD de Linux.
  - Se envían por red imágenes de cada dispositivo implicado a un equipo de recogida.

    ```
    dd id=/dev/hda | nc 192.168.1.2 12345
    ```

  - En el equipo de recogida, se recibe esta información y se almacena en disco.

    ```
    nc -l -p 12345 > hda.dd
    ```

  - Verificación (por ejemplo, comparar hash de original y copia).
  - Posteriormente, desglose de la imagen del dispositivo en imágenes de las particiones.

INETSECUR

Herramientas

- Herramientas
  - "Frameworks" completos:
    - Comerciales: Encase.
    - Libres: Autopsy, FLAG.
  - Aproximación minimalista: muchas herramientas pequeñas:
    - Rifiuti, Pasco, Galleta (libres): papelera de reciclaje, historial de IE5, cookies.
    - Microsoft Windows Event Viewer (comercial): visor de sucesos ;-)
    - Repertorio UNIX: dd, sha1sum, strings, grep, gdb...
    - SMART (comercial), AIR (libre): adquisición de datos.

Caso práctico

- IRIS-CERT (RedIRIS): Reto Análisis Forense
  - Invierno 2004.
  - Compromiso real de un sistema RH Linux 6.2.
  - Informe ejecutivo + informe técnico.
  - 14 participantes (individual o grupos).

INETSECUR

Referencias

- Reto IRIS-CERT: http://www.rediris.es/cert/ped/reto/
- The Honeynet Project: http://www.honeynet.org
- Herramientas
  - Sleuthkit, Autopsy: http://www.sleuthkit.org
  - PyFLAG: http://pyflag.sourceforge.net
  - Encase: http://www.encase.com
  - Rifiuti, Pasco, Galleta: http://www.foundstone.com
  - http://www.sysinternals.com

INETSECUR

Dudas y preguntas

Gracias por su asistencia

lgomez@inetsecur.com

INETSECUR