Coroner toolkit

IRIS-CERT <cert@rediris.es>

Martes 14 de Noviembre 2000

Capítulo 1

The Coroner toolkit

- Conjunto de herramientas de dominio publico para analizar un sistema.
- Realizado por Dan Farmer y Wietse Venema
- Disponible en http://www.porcupine.org o http://www.fish.com
- Solamente funciona en Unix
- No analiza los datos, solamente obtiene, información relevante para el análisis
- Incorpora un recuperador de ficheros borrados (lazarus) para cualquier Unix.
- Permite analizar los procesos en ejecución.

Capítulo 2

Experiencia

- Preparar una máquina “vulnerable” y atacarla, dejar rastros y ver como responde.
- Sistema Operativo muy viejo (RedHat 4.2) 1997
- Ataque contra el servidor de Imapd
- instalación del rootkit t0rn
- Problemas ;-)
  - Nunca instales un Unix antiguo en una máquina nueva.
  - El rootkit estaba compilado para Redhat 6.x , no funciona el login “troyano”.
  - El perl de RedHat 4.2 es muy viejo, no obtiene toda la información, pero es suficiente

Capítulo 3

Funcionamiento

- tct ya compilado antes
- Ejecución sobre otro Sistema de Ficheros (no modificar datos), mejor hubiera sido dd a otra máquina.
- Ejecución de “grave_robber” (30 Minutos, Pentium 166 100MB de HD ocupadas y el CDROM montado)
- Crea un directorio de datos con toda la información que obtiene
- Genera Hash MD5 de todos los ficheros (verificación)
- Obtiene información de todos los ficheros del equipo, incluidos los ocultos por el rootkit
- Genera “cores” de todos los procesos en ejecución para su análisis (pcat)
- Ficheros de configuración e historial de comandos de los usuarios

Capítulo 4

¿Qué encontró ?

- Listado de los ficheros ocultos por el rootkit
  - Buscar en los logs generados cadenas extrañas como se comento antes
- Información de las acciones realizadas por el atacante en el volcado de procesos
  - “strings sobre los cores”
- Por problemas con el Perl no se pudo realizar el análisis de fechas
  - Averiguar modificaciones de ficheros
  - Accesos a ficheros “anómalos” (compilación de programas).

Capítulo 5

Conclusiones

- Estupenda herramienta para automatizar la búsqueda de la información
- La información debe ser analizada después cuidadosamente.
- Debe ser complementada con otras (p.e.) rpm -qV
- Se puede pensar en tener un repositorio de binarios compilados e instrucciones.
- Documentación escasa.
- Hace 3 años Linux no estaba tan avanzado ;-(