Técnicas Forenses en Seguridad Informática

Luis Gómez Miralles

esCERT-UPC

Salamanca, 28 de octubre de 2004

Índice

1. Introducción
2. Marco legal
3. Adquisición de datos
4. Análisis
5. Caso práctico
6. Referencias

1. Introducción

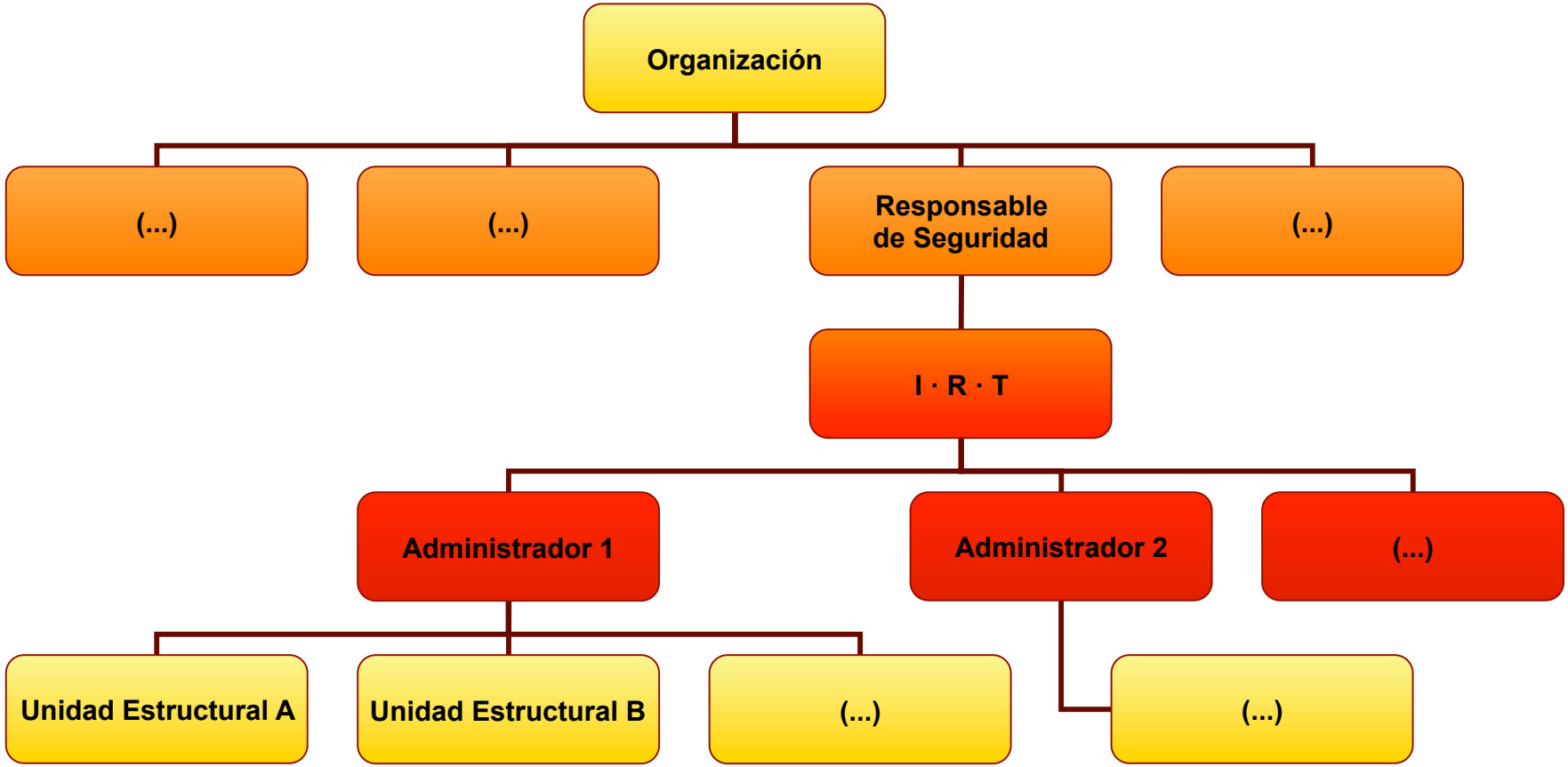
Definición

- Multitud de términos:
  - Análisis Forense (AF)
  - Análisis Post-Mortem
  - Investigación Digital
  - Evidencia Electrónica...
- Todos denotan más o menos lo mismo:
  - El análisis de información almacenada en la memoria (volátil o fija) de un dispositivo, a fin de poder extraer conclusiones en base a esa información, con garantías acerca de los resultados obtenidos.

Respuesta a Incidentes

- El AF cobra especial importancia en el marco de la Respuesta a Incidentes (RI).
- RI: administración centralizada de los incidentes de seguridad, internos y externos.
  - Permite gestionar la seguridad informática de la organización desde una perspectiva global.

IRT: Incident Response Team



Incident Readiness: capacidad de respuesta a incidentes

- Cuando (no si) nos comprometan un sistema, ¿qué querremos?
  - Saberlo lo antes posible: alerta temprana.
  - Obtener la máxima información sobre lo sucedido.
  - Con el mínimo coste (en tiempo, dinero, recursos en general).
  - Sin perder tiempo de servicio.

AF en el marco de la RI

- Motivación: obtener información acerca de lo ocurrido (por lo general, un incidente de seguridad).
  - Procedencia del incidente o ataque.
  - Punto de entrada.
  - Herramientas o medios utilizados.
  - Alcance dentro de nuestros sistemas.
  - Consecuencias

- Ayuda a la toma de decisiones en el marco de la Respuesta a Incidentes

Evidencia Digital

- ¿Qué es Evidencia Digital?
  - Una línea de texto en un log.
  - La hora de último acceso (*a-time*) 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.

Metodología

- **EP**: 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 del caso: escenario, actores, sistemas (fuentes de información relevantes).
- **AD**: Adquisición de datos
  - Copia de las fuentes de información relevantes.
  - Mecanismos para garantizar la preservación de la evidencia: hashes, timestamping.
- **AI**: Análisis e investigación
  - Se plantean teorías sobre lo sucedido. Según la evidencia encontrada, estas teorías se refuerzan o descartan.
- **PR**: Presentación
  - Exposición y defensa, ante un cliente o en un tribunal, de la validez de los resultados obtenidos.

Consideraciones

- Queremos garantías para nuestros resultados. Por tanto:
  - Todo el proceso debe estar perfectamente documentado.
    - ✓ Cualquier analista, partiendo de los datos originales y aplicando las técnicas y herramientas que hemos utilizado nosotros, deberá ser capaz de llegar a los mismos resultados.
  - Se debe contemplar desde el principio la legislación aplicable, así como las políticas de la Organización.

Herramientas

- Según su alcance:
  - Marcos enteros de trabajo, que abarcan cada fase del proceso.
  - Utilidades pequeñas (~ filosofía UNIX), con finalidades muy específicas, cada una útil en según qué campos.
- Según si son libres o no:
  - Productos de pago, generalmente de código cerrado.
  - Software libre: normalmente gratuito, y de código abierto.
  - En uno u otro caso es imprescindible acompañarlo con desarrollos propios.

- Como de costumbre, no hay una única solución. El analista debe conocer todas las herramientas disponibles, y utilizar las que más se adecuen a cada caso.

2. Marco legal

Órdenes jurídicos

- Procedimientos laborales
- Procedimientos civiles
- Procedimientos penales

Consideraciones

- **Proporcionalidad:** se recomienda no recoger más datos de los estrictamente necesarios para probar aquello que es objeto de estudio. Ejemplos:
  - e-mail: recoger y analizar sólo cabeceras de los mensajes.
  - Transferencias ilícitas de ficheros: registrar sólo origen y destino, nombre y tamaño del archivo, y quizá un hash.
  - Navegación abusiva en horas de trabajo: apuntar sólo las direcciones que el empleado visita y las franjas horarias en que lo hace, sin entrar en principio a valorar su contenido.

Consideraciones

- Cuando no es posible hacer una recogida selectiva de datos, ***podría*** ser aceptable el uso de técnicas indiscriminadas (xej. instalación de un sniffer) siempre que después los resultados sean filtrados por procesos automáticos para, sin violar el secreto de las comunicaciones personales, llegar a encontrar aquella información que es objeto de la investigación.

Procedimientos laborales

- Aquellos procedimientos en que existe una relación laboral entre las partes denunciante y denunciada.
- Se limita la capacidad de control del empresario, en favor de los derechos fundamentales de los trabajadores.
- No obstante, existen sentencias dispares acerca del derecho del empresario a inspeccionar o monitorizar los equipos de los trabajadores.

Procedimientos laborales

- Art. 90.1 LPL:
  - "Las partes podrán valerse de **cuantos medios de prueba se encuentren regulados en la Ley**, admitiéndose como tales los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, **salvo que se hubieran obtenido**, directa o indirectamente, **mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas**."

Procedimientos laborales

- En los registros de equipos informáticos de los empleados, se recomienda respetar **como mínimo** los mismos principios que atañen a sus taquillas. Así, el registro debe realizarse:
  - En horario de trabajo.
  - Dentro de los locales de la empresa.
  - En presencia de un representante de los trabajadores.

3. Adquisición de datos

Adquisición de datos

- De cada sistema objeto de estudio, copia de la información relevante para el caso.
  - Contenida en soportes no volátiles.
  - Contenida en soportes volátiles (hasta donde sea posible).
- Apagar o no apagar, he ahí el dilema...
  - Sin apagar, pueden verse 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.

Herramientas

- Aproximación minimalista: Arrancar el sistema en un entorno controlado (xej LiveCD de Linux)
  - Enviar imágenes de cada dispositivo por red:

    ```
    dd if=/dev/hda | nc 192.168.1.190 12345
    ```

  - En el equipo de recogida, se almacena esa información:

    ```
    nc -l -p 12345 > /mnt/morgue/hda.dd
    ```

  - Validez de la prueba: verificación (hashes SHA-1 o MD5 de original y copia). A poder ser, timestamping.
- Aproximación "moderna": SMART (de pago), AIR (libre), o la función de Adquisición en paquetes como Encase o FTK.

4. Análisis

Aproximación tradicional

- Fuentes de información:
  - Logs (del sistema analizado, de otros próximos o en su perímetro...).
  - Captuas del tráfico de red (de IDSs, completas, etc.).
  - Ficheros del sistema analizado:
    - ✓ Ingeniería inversa de binarios
    - ✓ mac-times
- Temporalización → **Correlación**.

Ejemplo de timeline (1/3)

Ejecución de *adduser EVIL*

TAMAÑO		UID	GID	I-NODE	FICHERO
7	.a.	root	root	158994	/usr/sbin/adduser -> *useradd*
52348	.a.	root	root	159006	/usr/sbin/useradd
96	.a.	root	root	40163	/etc/default/useradd

Modificación de *gshadow*, *group* y *lastlog*

TAMAÑO		UID	GID	I-NODE	FICHERO
400	m..	root	root	28263	/etc/gshadow-
400	m..	root	root	28264	*<hda8.dd-dead-28264>*
484	m..	root	root	26151	/etc/group-
146584	m.c	root	root	12050	/var/log/lastlog

Creación del *home* y copia de *skel*

TAMAÑO		UID	GID	I-NODE	FICHERO
4096	m.c	EVIL	EVIL	63361	/home/EVIL
124	.a.	root	root	40166	/etc/skel/.bashrc
124	mac	EVIL	EVIL	63364	/home/EVIL/.bashrc
224	.a.	root	root	40165	/etc/skel/.bash_profile
224	mac	EVIL	EVIL	63363	/home/EVIL/.bash_profile

Ejemplo de timeline (2/3)

Lectura de opciones *PAM*, y solicitud de password

TAMAÑO		UID	GID	I-NODE	FICHERO
210	.a.	root	root	60254	/etc/pam.d/other
211	.a.	root	root	60256	/etc/pam.d/passwd
637	.a.	root	root	60255	/etc/pam.d/system-auth
14764	.a.	root	root	6039	/lib/security/pam_cracklib.so
5046	.a.	root	root	6040	/lib/security/pam_deny.so
13137	.a.	root	root	6041	/lib/security/pam_env.so
13858	.a.	root	root	6047	/lib/security/pam_limits.so
10874	.a.	root	root	6060	/lib/security/pam_stack.so
46971	.a.	root	root	6064	/lib/security/pam_unix.so
19	.a.	root	root	44255	/lib/libpam_misc.so.0 -> *(ídem.0.74)*
12191	.a.	root	root	44254	/lib/libpam_misc.so.0.74
17	.a.	root	root	44248	/lib/libpwdb.so.0 -> *(ídem.0.61.1)*
133705	.a.	root	root	44247	/lib/libpwdb.so.0.61.1
15	.a.	root	root	174499	/usr/lib/libcrack.so.2 -> *(ídem.2.7)*
70446	.a.	root	root	174498	/usr/lib/libcrack.so.2.7
13536	.a.	root	root	159701	/usr/bin/passwd

Ejemplo de timeline (3/3)

Aplicación de *libcrack*

TAMAÑO		UID	GID	I-NODE	FICHERO
1024	.a.	root	root	175310	/usr/lib/cracklib_dict.hwm
42116	.a.	root	root	175312	/usr/lib/cracklib_dict.pwi
828334	.a.	root	root	175311	/usr/lib/cracklib_dict.pwd

Modificación final de *shadow* y *passwd*

TAMAÑO		UID	GID	I-NODE	FICHERO
856	m..	root	root	28261	/etc/shadow-
1044	m..	root	root	28123	/etc/passwd-
1044	m..	root	root	28265	*<hda8.dd-dead-28265>*

Un paso más...

- La información obtenida "en vivo" puede ser muy valiosa si podemos asegurar su veracidad:
  - Conexiones de red abiertas: ¿desde / hacia dónde?
  - Usuarios conectados en la máquina.
  - Procesos en ejecución.
  - Tablas ARP, de rutas, y otras cachés.
  - Filesystems temporales.

- Queda mucho por hacer en este campo.

El proceso de análisis

- Se van correlando partes de la información recogida para formular hipótesis.
  - En base al resto de información, estas hipótesis se refuerzan o descartan.
- Finalmente se encadenan las hipótesis obtenidas y se les da veracidad apoyándolas en los datos recogidos.

Herramientas

	Entornos completos	Herramientas minimalistas
Software libre	TCT → Sleuthkit Autopsy (py)FLAG	Rifiuti (papelera) Pasco (historial IE) Galleta (cookies IE)
Software cerrado	Guidance SW: Encase AccessData: FTK	(...)

5. Caso práctico

La herramienta

- Sleuthkit:
  - Conjunto de herramientas derivado de TCT.
  - Funciona sobre UN*X.
  - Filesystems soportados: FAT, NTFS, ext2/3, FreeBSD, OpenBSD, Solaris.
- Autopsy:
  - Frontal web a Sleuthkit.

http://www.sleuthkit.org

Gestión de casos

- Caso A:
  - Máquina A1:
    - ✓ Imagen A1a.
    - ✓ Imagen A1b.
  - Máquina A2:
    - ✓ Imagen A2a.
- Caso B:
  - (...)

- Opciones de Sleuthkit:
  - New case
    - ✓ Add host
      - o Add image
  - Open case

Opción “New case”

- Nombre.
- Texto descriptivo.
- IDs de los analistas.
  - A fin de registrar sus acciones en los logs.

Opción “Add host”

- Nombre.
- Texto descriptivo.
- Zona horaria.
  - Para poder correlar información de máquinas en diferentes zonas.
- Desfase del reloj.
  - Por si las distintas fuentes de información no están sincronizadas.
- Bases de datos “bueno/malo”.
  - En desuso actualmente (en este producto).

Opción “Add image”

- Ruta a la imagen.
- Modo de importarla: copiar, mover, enlazar.
- Sistema de archivos.
- Punto de montaje en el sistema original.
- Opciones para asegurar la integridad.

Modos de análisis

- File Analysis: Examinar ficheros y directorios.
  - También muestra ficheros borrados.
- Keyword Search: búsqueda de cadenas.
- File Type: analizar los tipos de ficheros (y ordenarlos).
  - Permite previsualizar las imágenes, detectar estenografía débil...
- Image Details: muestra detalles sobre la imagen.
- Meta Data: exploración por metadatos (por inodo, por entrada FAT, por entrada MFT...)
- Data Unit: exploración por cluster.

Otras características

- Notas.
- Event Sequencer (notas fechadas).
- Timeline (correlación de *mac-times*).

El caso

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

http://www.rediris.es/cert/ped/reto/

http://www.rediris.es/cert/ped/reto/resultados.html

Indicios significativos

- Sobre la timeline:
  - 00:21h: Intrusión por FTP desde 200.47.186.114 según consta en /var/log/secure, /var/run/ftp.rips-all y /var/log/ messages .
  - 00:24h: Creación de /var/ftp/nerod.tar.gz
  - 00:25h: Comienza la troyanización.
  - ...

6. Referencias

- Documentación
  - www.honeynet.org
  - www.htcia.org
  - www.ctose.org
- Herramientas
  - www.sleuthkit.org
  - www.foundstone.com
  - www.atstake.com
  - chiht.dfn-cert.de

¡Gracias por su asistencia!

lgomez@inetsecur.com