Computo Forense

Un acercamiento

Juan Manuel López Villalobos
Sistemas de Información, UABC
mlopez@uabc.mx
Grupo de seguridad de RedCUDI

Introducción

- Uso generalizado de sistemas y equipos de computo
- Derivado de esto también surge el uso para fines criminales o no éticos
- El uso de todo sistema de computo deja rastros

Introducción

- “Nueva” área en seguridad computacional
- Considerada una ciencia
- No remplaza a una estrategia de seguridad

Definiciones

- Se refiere a la adquisición, análisis y presentación de evidencia para reconstruir información o eventos relacionados con un incidente de seguridad o crimen informático
- No es solo localizar información borrada o recuperarla de un archivo

Definiciones

- Crimen informático, cualquier ofensa, actividad o evento relacionado con algún equipo de computo
- El equipos de computo es la herramienta
- El equipo de computo es la victima

Definiciones

- Incidente de seguridad, evento donde la política de seguridad es desobedecida o quebrantada

Objetivos

Ayudar a definir:

- Que paso?
- Como sucedió?
- Cuando ocurrio?
- Quien lo hizo?

Donde se utiliza

- Sector Publico: Gobiernos y cuerpos policíacos, para investigar crímenes “tradicionales”
- Sector Privado: Para investigar accesos no autorizados, uso inapropiado de recursos de computo, robo o destrucción de P.I., robo de información secreta, fraudes

Metodología Básica

- Identificación
- Adquisición
- Análisis
- Presentación

Identificación

- Identificar y registrar toda posible evidencia; marcas, modelos y números de serie, mantener una copia con la evidencia
- Posibles fuentes de evidencias: Discos duros, floppy disk, zip disk, cintas magneticas, CD, PDA, Appliances: routers, switches, etc.

Identificación

- Cadena de custodia: Quien, Que, Donde, Cuando, Porque, Como, mantener una copia con la evidencia
- Donde, cuando y quien fue el primero en tener contacto con la evidencia
- Donde, cuando y quien examino la evidencia

Identificación

- Quien tiene la custodia y por cuanto tiempo
- Como fue almacenada
- Cuando hubo cambio de custodia, cuando y como se hizo la transferencia

Adquisición

- Adquirir la evidencia sin alterarla o dañarla
- Autentificar que la información de la evidencia obtenida es igual a la original
- Obtener información de fuentes adicionales

Adquisición

Orden de adquisicion:

- Registros, cache
- Tablas de ruteo, arp cache, lista de procesos, información del kernel memoria
- Sistemas de archivos temporales
- Discos
- Registros remotos e información de monitoreo relevante
- Información almacenada

Adquisición

- Autentica
- Correcta
- Completa
- Convincente
- En caso de una acción legal, admisible

Análisis

- Es necesario conocer a la victima
- Analizar la información sin modificarla
- Identificar los archivos en la evidencia: normales, borrados, pedazos, protegidos, encriptados

Análisis

- Recuperar posibles datos relevantes, como: archivos borrados, archivos ocultos
- Revelar el contenido de archivos ocultos, temporales, swap, encriptados o con password

Análisis

Tres tipos de datos :

- Datos activos
- Datos almacenados
- Datos latentes

Análisis

Donde buscar:

- Correos electrónicos
- Directorios Temp
- Recycle Bin
- Recent Files
- Spool files
- Historial de acceso a Internet
- My Documents
- Favorites / Bookmarks

Análisis

Donde buscar:

- /etc
- /bin, /sbin, /usr/bin, /usr/sbin
- /var/[spool| log| adm| www| …]
- /home
- suid,
- .*, ..*
- /proc, /tmp, /dev

Presentación

- Reporte explicito de la investigación
- Listado de archivos y datos encontrados
- Intentos de ocultar, borrar o proteger información

Presentación

- Todo aquello que se descubrió y pueda ser relevante
- Posible autor y sus acciones

Aspectos legales

- Computo forense desconocido por la Ley
- Posible aplicación “no oficial” del computo forense
- Código de Comercio, Ley de Instituciones de Crédito, Ley del Mercado de Valores y Código Federal de Procedimientos Civiles

Aspectos legales

- Fraude, Art. 230 -231 Código penal para el D.F.
- Acceso no autorizado a sistemas o servicios y destrucción de programa o datos, Art 221 bis1 a 211 bis 7 Código Penal Federal
- Reproducción no autorizada de programas informáticos, Ley Federal del Derecho de Autor

Aspectos legales

- Uso no autorizado de programas y de datos, LFDA, Ley de Protección de Datos Personales del Estado de Colima
- Obtención o interferencia de información que viaja por una red, Art. 167 Fr VI Código Penal Federal

Consejos / Tips

- Ser imparcial. Solamente analizar y reportar lo encontrado
- Nunca realizar una investigación formal sin experiencia
- Mantener la cadena de custodia
- Documentar toda actividad realizada

Consejos / Tips

- Los medios de almacenamiento deberán ser “esterilizados”
- Si esta prendido, no apagarlo
- Si esta apagado, no prenderlo
- Pensar como el intruso o criminal

Consejos / Tips

- Conocer el funcionamiento del HW y SW
- Conocer las herramientas a utilizar
- PACIENCIA

GRACIAS

Juan Manuel López Villalobos
Sistemas de Información, UABC
mlopez@uabc.mx
Grupo de seguridad de RedCUDI