Cómputo Forense

Diciembre 2016

Introducción

- Es un área que forma parte de la seguridad informática que ha emergido por el aumento de incidentes que comprometen a un sistema
- El análisis forense generalmente es realizado una vez que el incidente ocurrió
- El análisis forense consiste en reconstruir cómo fue vulnerado un sistema informático

Interrogantes

- Cuando un análisis forense es realizado el experto debe responder las siguientes interrogantes:
  - ¿Quién realizó el ataque?
  - ¿Cómo lo realizó?
  - ¿Qué vulnerabilidades se han explotado?
  - ¿Qué hizo el intruso una vez dentro del sistema?

Incidente de seguridad

- Es cualquier acción fuera de la ley o no autorizada, como por ejemplo:
  - Ataques de denegación de servicio
  - Extorsión
  - Envío de correos electrónicos ofensivos
  - Fuga de información confidencial dentro de una organización

Fuentes de información para realizar un análisis forense

- Correos electrónicos
- IDS (sistemas de detección de intrusos)
- Archivos de bitácoras de los firewalls
- Archivos de bitácora de acceso al sistema
- Entrevistas con responsables de seguridad y administradores de sistemas

Metodología

- **1) Preparación y prevención**
  - Tomar acciones para preparar a la organización antes de que ocurra un incidente
- **2) Detección del incidente**
  - Clasificando los incidentes como: accesos no autorizados, código malicioso para provocar una infección, denegación de servicio, suplantación de identidad
- **3) Respuesta inicial**
  - Entrevistas con administradores, revisión de topologías de red, entrevista con personal y revisión de bitácoras. Se entrega un primer reporte con fecha y hora del incidente, tipo, hardware, software, cuándo ocurrió
- **4) Formulación de una respuesta**
  - Una vez recabada la información anterior, esta se analiza para tomar una decisión sobra la acción a ejecutar, p.ej. Si un sitio Web ha sido atacado o modificado, se recomendaría hacer un monitoreo, e investigación online mientras esté activo
- **5) Investigación del incidente**
  - Se determina quién, cuándo, dónde, qué y cómo, y por qué ocurrió el incidente, **análisis forense**
- **6) Redacción del informe**
  - Se prepara un documento que debe ser entregado a la dirección de la empresa u organización. Tiene dos vistas: una ejecutiva y otra técnica

Análisis forense

- ¿Qué se analizaría?
  - Sistemas: servidores y estaciones de trabajo
  - Redes: cableadas, inalámbricas (direcciones registradas)
  - Sistemas embebidos: en casos que el incidente involucre dispositivos móviles

Fases de un análisis forense

- **1) Adquisición de datos**
  - Es una fase delicada, si es realizada incorrectamente, el análisis o investigación estaría comprometida
  - ¿Apagar o no el equipo?
    - En caso de ser apagado se puede perder evidencias disponibles en la memoria volátil:
      - Conexiones abiertas
      - Procesos en ejecución
      - Información de la RAM
  - En esta parte es necesario clonar discos duros

Fases de un análisis forense

- **2) Adquisición e investigación**
  - Bitácoras de los sistemas
  - Detectores de intrusión
  - Firewalls
  - Archivos de sistema
  - Evitar revisión de carpetas personales de los usuarios: /home/…

Fases de un análisis forense

- **3) Redacción del informe**
  - Con evidencias recopiladas, se deben explicar de una forma sencilla y clara, considerando que las personas que leen los informes no tienen conocimientos técnicos, sin embargo, deben ser estrictamente rigurosos
  - Debe mencionar la fecha de finalización de la investigación, además de las personas involucradas
    - Ejecutivo
      - Sin contemplar un perfil técnico, contienen: Introducción, Descripción (lo sucedido), Recomendaciones (acciones a realizar),
    - Técnico
      - Orientado a ingenieros y técnicos, contiene: Introducción, Preparación del entorno (cómo recuperar los datos para la replicación y verificación del equipo o sistema afectado), Estudio forense de las evidencias, Conclusiones

Herramientas

- **Captura de tráfico**
  - Wireshark
  - Tcpdump
- **Editores**
  - WinHex
- **Virtualización**
  - Xen
  - VMWare
- **Análisis e investigación**
  - Autopsy
  - Encase Forensic
- **Clonación de dispositivos**
  - dd
  - Ghost