Computer Forensics

Análisis Forense Informático

El análisis forense de ordenadores es una de las áreas de la seguridad informática que más ha evolucionado en los últimos años, siendo además una de las grandes desconocidas. Uno de sus principales objetivos es responder a las preguntas que se plantean cuando se descubre que un atacante ha conseguido acceder a uno o varios de los equipos de una empresa u organismo: ¿Quién ha realizado el ataque?, ¿Cómo se realizó?, ¿qué vulnerabilidad se empleó? ¿Qué hizo el atacante cuando accedió al sistema?, etc...

Ondata International realiza el **análisis forense en equipos informáticos** que han sido previamente atacados y en los cuales el atacante ha conseguido tener un control total del equipo. Mediante el análisis forense informático se estudian las acciones realizadas por los usuarios (ficheros copiados, leídos, borrados, programas ejecutados, etc.) y así poder reconstruir las acciones ejecutadas por los atacantes.

A este proceso se le conoce como análisis forense informático debido a sus similitudes con una autopsia real realizada en investigaciones policiales. Los pasos que se siguen son:

1. "Congelar la escena", es decir, realizar una copia del estado en el que se encuentran los sistemas atacados, de forma que se puedan "preservar" las evidencias.

2. Descubrir los programas que fueron ejecutados, los datos leídos, los modificados...

3. Indicar la secuencia de acciones que realizó el atacante en el equipo y recons- truir así las acciones que llevó a cabo.
4. Identificar, en su caso, al responsable del ataque informático a través de sus huellas virtuales.

Este análisis forense informático tiene utilidades en el campo de la seguridad empresarial, así como en investigaciones sobre delitos informáticos y búsqueda de pruebas, huellas o indicios delictivos.

Sin embargo hay una **preocupación generalizada por la aparente vulnerabilidad del acceso a la información** por parte de cualquier empleado descontento o de un hacker. Se teme que se pueda borrar o sustraer información por parte de personas no autorizadas o aún cuando autorizados, puedan hacer un mal uso de la misma..

Aún cuando la mencionada vulnerabilidad es aparente, existen **medios para poder investigar** estas posibles intrusiones y poder llegar a recuperar esta información si ha sido destruida, o a conclusiones de quién, cuando y como ha hecho un uso no autorizado de la información.

Computer Forensics

ondata INTERNATIONAL