Análisis forense de sistemas de información

Investigación de la evidencia digital

Jordi Serra Ruiz (coordinador)
Miguel Colobran Huguet
Josep María Arqués Soldevila
Assumpció Guasch Petit

PID_00146433

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Jordi Serra Ruiz

Ingeniero informático por la Universidad Autónoma de Barcelona (UAB). Máster en Informática industrial por la UAB. Profesor del Departamento de Informática de la UAB hasta el 2002. Actualmente, es profesor de la Universitat Oberta de Catalunya (UOC) y es el director académico del máster de Seguridad informática de la UOC.

Miguel Colobran Huguet

Licenciado en Informática por la Universidad Autónoma de Barcelona. Elaboró su trabajo de investigación en el Departamento de Ingeniería de la Información y de las Comunicaciones (DEIC) de la misma Universidad. Ha trabajado como profesor ayudante y asociado en el DEIC, y ha ejercido de consultor de varias asignaturas de la Universitat Oberta de Catalunya. Actualmente, trabaja como analista en informática forense.

Josep María Arqués Soldevila

Licenciado en Informática por la Universidad Autónoma de Barcelona en 1991. Ha hecho el trabajo de investigación en el Departamento de Ingeniería de la Información y de las Comunicaciones (DEIC) de esta Universidad. Consultor en la UOC durante varios años de asignaturas como *Fundamentos de computadores I y II*, y *Sistemas operativos I en informática*.
Autor de diferentes cursos de administración de sistemas operativos (Solaris, Windows NT, etc.), ha dirigido el departamento de informática de una empresa durante tres años. Actualmente, forma parte de diferentes departamentos de la Universidad Autónoma, donde trabaja en la gestión informática y la administración de los sistemas, siempre con un trato directo y atención final a los usuarios.

Assumpció Guasch Petit

Técnica superior diplomada en Informática (UAB), máster en Tecnologías de seguridad informática (ICT/esCERT-UPC), auditora informática (UPC) y auditora por BS 7799 en seguridad de SI (BSI). Ha participado en cursos y seminarios especializados en peritajes informáticos e informática forense. Ha trabajado como profesional informática en varias empresas y como consultora de la UOC. Asimismo, es autora de diferentes publicaciones y actualmente ejerce como perito judicial y consultora informática.

Primera edición: septiembre 2009
© Jordi Serra Ruiz, Miguel Colobran Huguet, Josep María Arqués Soldevila, Assumpció Guasch Petit
Todos los derechos reservados
© de esta edición, FUOC, 2009
Av. Tibidabo, 39-43, 08035 Barcelona
Diseño: Manel Andreu
Realización editorial: Eureca Media, SL
Depósito legal: B-31.001-2009

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares del copyright.

Agradecemos a la UCIF (Unitat Central d'Informàtica Forense dels Mossos d'Esquadra de la Generalitat de Catalunya) su colaboración en la elaboración de estos materiales.

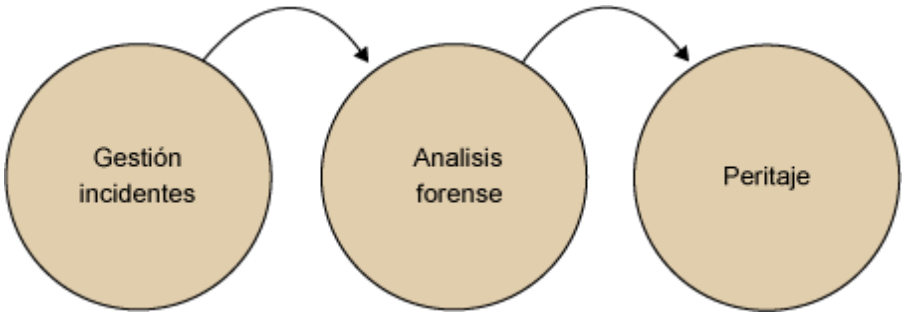
Introducción

Hoy en día, cualquier organización cuenta con sistemas informáticos. Éstos estarán conectados formando una red y, de alguna forma, lo estarán con la red de redes: Internet. En este entramado, veremos PDA, portátiles, ordenadores de sobremesa, servidores, móviles con tecnología inalámbrica y un sinfín de dispositivos (USB, *firewire*, *bluetooh*, etc.) que nos proporcionarán un paisaje muy flexible y dinámico, a la par que vulnerable.

Mantener el correcto control de acceso y uso de la información se convierte en una tarea compleja y no exenta de riesgos. Con la gestión de incidentes, haremos todo lo posible por evitar que dichos riesgos se materialicen. Sin embargo, tarde o temprano, alguien puede encontrar algún resquicio en el sistema defensivo y provocar daños o robar información (bienes intangibles) en su propio provecho. Estaremos, entonces, ante un incidente de seguridad.

La informática forense se convierte, a partir de este momento, en la herramienta estrella: recoge información digital sobre el incidente, la analiza y determina lo que ha sucedido. Para ello, se sirve de aplicaciones y tecnologías que sean aceptadas en los tribunales, con el propósito de presentar dicha información como evidencias en un informe pericial.

Este procedimiento puede esquematizarse de la manera siguiente:



Mediante la gestión de incidentes se hará todo lo posible para evitar que ocurra cualquier problema en el sistema informático. Nos prepararemos para evitar el suceso y para que, si algo ocurre, podamos actuar rápida y eficazmente.

Análisis forense: por muchas precauciones que se tomen, tarde o temprano se producirá un incidente a tratar, de modo que se deberá investigar con el fin de descubrir qué ha ocurrido (su origen, qué ha dañado, por dónde se ha expandido, etc.).

Peritaje: con todas las evidencias digitales recogidas, y si debemos actuar legalmente, hay que preparar un informe pericial, presentarlo ante un tribunal y defenderlo con las debidas garantías.

Los materiales describen en profundidad la metodología de análisis forense como uno de sus objetivos principales. Sin embargo, estamos convencidos de que dotar estos materiales de un marco de aplicación, como por ejemplo, la gestión de incidentes, facilita la comprensión de la materia, e incluso permite que estas técnicas puedan ser usadas por el estudiante en su entorno laboral.

Objetivos

Competencias

Esta asignatura contiene los materiales didácticos necesarios para que el estudiante aprenda, desarrolle y asimile los siguientes conocimientos y habilidades:

1. Conocer la metodología de la informática forense y cómo aplicarla.

2. Saber identificar en qué situaciones la informática forense resulta de utilidad.

3. Conocer de qué manera las diferentes técnicas forenses se relacionan con los sistemas informáticos.

4. Saber aplicar la metodología forense en la preparación del informe pericial para su uso ante un tribunal de justicia.

5. Conocer cómo se relaciona la informática forense con la gestión de incidentes.

6. Saber preparar la gestión de incidentes de una organización correctamente para minimizar los ataques exitosos.

7. Comprender cómo la informática forense ayuda a mantener y reforzar la seguridad del sistema informático.

Contenidos

Bibliografía

Casey, E. (2004). *Digital Evidence and Computer Crime*. Elsevier.

Colobran Huguet, M.; Moron Lerma, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC S. L.

Cruz Allende, D. (2007). *Análisis forense de sistemas de información*. FUOC.

IETF (2002). Guidelines for Evidence Collection and Archiving (RFC 3227) <http://www.ietf.org/rfc/rfc3227.txt>

Barbara, J. (ed.) (2008). *Handbook of Digital and Multimedia Forensic Evidence*. Humana Press Inc.

Kent, K.; Chevalier, S.; Grance, T.; Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. U.S. Department of Commerce: Nist, National Institute of Standards and Technology.
<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

Microsoft Technet (2009). *Respuesta a incidentes de seguridad de TI.*
<http://technet.microsoft.com/es-es/library/cc700825.aspx>

Ministerio de Administraciones Públicas (2006). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (versión 2). Madrid: MAGERIT.
<http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf>

Serra Ruiz, J.; Colobran, M.; Arqués, J.M. y Marco, E. (2009). *Administració de xarxes i sistemes operatius*. FUOC.

West-Brown, M.; Stikvoort, D.; Kossakowski, K.;Killcrece, G.; Ruefle, R. and Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)*. U.S. Carnegie Mellon University. <http://www.cert.org/archive/pdf/csirt-handbook.pdf>