Análisis Forense de Sistemas Informáticos

Curso Académico: (2021 / 2022) **Fecha de revisión: 29-06-2021**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PERIS LOPEZ, PEDRO

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No procede

OBJETIVOS

Se definen los siguientes objetivos en términos de resultados de aprendizaje, acorde al nivel de Máster definido en el RD 1027/2011, de 15 de julio, y al ámbito de la informática forense.
El estudio de esta asignatura lleva a la obtención de las siguientes competencias básicas:
- Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación (CB6).
- Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio (CB7).
- Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios (CB8).
- Que los estudiantes sepan comunicar sus conclusiones ¿y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades (CB9).
- Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo (CB10).
Así mismo, el alumno también adquirirá las siguientes competencias generales y específicas.
- Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido (CG2)
- Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad (CG3)
- Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad (CG4)
- Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias (CE4)

A la superación de esta materia y como resultado del aprendizaje, los estudiantes deberán ser capaces de:
- Diseñar estrategias de sensorización para distintos elementos de un sistema en red y analizar los eventos observados en un ataque concreto para distinguir cuáles son de interés.
- Dado un sistema bajo distintos tipos de ataques, ser capaz de detectar las características de la mayoría de dichos ataques y señalar las fuentes más probables.
- Dado un sistema atacado, encontrar algunas de las evidencias del ataque y explicar las medidas necesarias para mantener la cadena de custodia de dichas evidencias.
- Conocer la normativa legal y técnica de aplicación en el marco de la ciberseguridad.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Análisis Forense de Sistemas Informáticos:

1. Introducción al Análisis Forense
1.1. ¿Qué es la informática forense?
1.2. Casos de ejemplo
1.3. Conceptos técnicos clave

2. Laboratorio de Análisis Forense
2.1. Laboratorio

2.2. Políticas y procedimientos
2.3. Garantía de la calidad
2.4. Herramientas
2.5. Evidencias: obtención, análisis y custodia
2.6. Informe forense

3. Herramientas de Análisis Forense
3.1. Análisis forense de sistemas de ficheros
3.2. Análisis forense de memoria
3.3. Análisis forense en redes de ordenadores
3.4. Internet y correo electrónico
3.5. Análisis forense en dispositivos móviles
3.6. Herramientas y técnicas anti-forense

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La metodología docente se basa en la aplicación en vivo de los conceptos clave que se presentan a lo largo de la asignatura, para lo cual se hará uso de una colección de ejercicios que servirán como base para la explicación correspondiente a cada sesión. Además de esto, los alumnos deberán llevar a cabo de manera autónoma diferentes casos prácticos de análisis forense. Como parte de su trabajo, los alumnos deberán realizar un análisis crítico de los informes entregados por otros compañeros.
Así, la metodología se concreta en:
- MD1. Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
- MD2. Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
- MD3. Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.
- MD4. Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos.
- MD5. Elaboración de trabajos e informes de manera individual o en grupo.

SISTEMA DE EVALUACIÓN

El sistema de evaluación se basa en la realización de ejercicios prácticos de manera individual y en grupo, además de un examen final. Específicamente, la evaluación de la asignatura se desglosa en:

Trabajos prácticos periódicos (90% de la nota final) [SE2]

Realización de trabajos prácticos de entrega periódica (e.g. semanal) relativos al tema estudiado en cada sesión. El trabajo podrá abarcar la crítica y análisis de trabajos realizados por otros compañeros.

Examen final (10% de la nota final) [SE3]

De carácter teórico-práctico, podrá incluir casos prácticos para desarrollar.

Para la superación de la asignatura será necesario superar el examen final (es decir, calificación mínima de 1.25 sobre 2.5 puntos), y obtener, como mínimo, 5 puntos sobre 10 en el total.

En la convocatoria extraordinaria, y salvo indicación en contrario al comienzo de la asignatura, no se autoriza la re-entrega de ejercicios de evaluación continua.

Peso porcentual del Examen Final:	10
Peso porcentual del resto de la evaluación:	90

BIBLIOGRAFÍA BÁSICA

- Aaron Phillip; David Cowen, Chris Davis Hacking Exposed: Computer Forensics (ISBN 0071626778), McGraw Hill Professional, 2009
- Andy Jones and Craig Valli Building a digital forensic laboratory, Syngress, 2011
- Casey, E. Handbook of Digital Forensics and Investigation (ISBN 0123742676), Academic Press. , 2009
- Casey, Eoghan Digital Evidence and Computer Crime, Third Edition, Elsevier, 2012

- John Sammons The basics of digital forensics, Syngress, 2012

- K S Rosenblatt High-Technology Crime: Investigating Cases Involving Computers, KSK Publications, 1995

- Kruse, W. & Heiser, J. Computer forensics: incident response essentials, Addison Wesley, 2002

- Marcella, A. & Greenfield Cyber forensics: A field manual for the collecting, examining, and preserving evidence of computer crimes, CRC Press, 2002

- Shinder, D Scene of the cybercrime: Computer forensics handbook, Syngress, 2002

- US Department of Justice Searching & seizing computers and obtaining electronic evidence in criminal investigations., Computer crime & intellectual property section US DoJ, 2001

BIBLIOGRAFÍA COMPLEMENTARIA

- Vrizlynn L.L. Thing, Kian-Yong Ng, Ee-Chien Chang Live memory forensics of mobile phones, doi:10.1016/j.diin.2010.05.010. ISSN 1742-2876, 2010

RECURSOS ELECTRÓNICOS BÁSICOS

- Safari Books Online . Proquest: //proquest.safaribooksonline.com

- n.a. . Forensic Wiki: //www.forensicswiki.org/wiki/Main_Page