Universitat de Lleida

GUÍA DOCENTE

SEGURIDAD DE APLICACIONES Y COMUNICACIONES

Coordinación: FERNANDEZ CAMON, CESAR

Año académico 2017-18

SEGURIDAD DE APLICACIONES Y COMUNICACIONES 2017-18

Información general de la asignatura

Denominación	SEGURIDAD DE APLICACIONES Y COMUNICACIONES
Código	102028
Semestre de impartición	1R Q(SEMESTRE) EVALUACIÓN CONTINUADA
Carácter	<table><tr><th>Grado/Máster</th><th>Curso</th><th>Carácter</th><th>Modalidad</th></tr><tr><td>Grado en Ingeniería Informática</td><td>4</td><td>OBLIGATORIA</td><td>Presencial</td></tr></table>
Número de créditos ECTS	9
Grupos	1GG
Créditos teóricos	6
Créditos prácticos	3
Coordinación	FERNANDEZ CAMON, CESAR
Departamento/s	INFORMATICA I ENGINYERIA INDUSTRIAL,MATEMATICA
Distribución carga docente entre la clase presencial y el trabajo autónomo del estudiante	9 ECTS = 25x9 = 225 horas de trabajo 40% --> 90 horas presenciales 60% --> 135 horas de trebajo autónomo
Información importante sobre tratamiento de datos	Consulte este enlace para obtener más información.
Idioma/es de impartición	Catalán / Inglés Materiales en Inglés
Distribución de créditos	FERNANDEZ CAMON, CESAR, 3ECTS MATEU PIÑOL, CARLOS, 3ECTS

SEGURIDAD DE APLICACIONES Y COMUNICACIONES 2017-18

Profesor/a (es/as)	Dirección electrónica profesor/a (es/as)	Créditos impartidos por el profesorado	Horario de tutoría/lugar
FERNANDEZ CAMON, CESAR	cesar@diei.udl.cat	3	
MARTÍNEZ RODRÍGUEZ, SANTIAGO	santi@matematica.udl.cat	3	
MATEU PIÑOL, CARLOS	carlesm@diei.udl.cat	3	

Información complementaria de la asignatura

Para cursar la asignatura se requieren conocimientos previos de sistemas operativos, programación y redes y comunicaciones.

Objetivos académicos de la asignatura

- Entender los conceptos, problemas y procedimientos de seguredad informática
- Elaborar auditorias de seguredad sencillas
- Entender los conceptos y mecanismos básicos de la criptografía y autenticación
- Diseñar esquemas de cortafuegos
- Desarrollar aplicaciones en entornos de comunicación seguros

Competencias

CT2. Adquirir un dominio significativo de una lengua extranjera, especialmente del inglés

CT3. Adquirir capacitación en el uso de las nuevas tecnologías y de las tecnologías de la información y la comunicación

GII-TI2. Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.

GII-TI6. Capacidad de concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil.

GII-TI7. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

EPS11 Capacidad de comprender las necesidades del usuario expresadas en un lenguaje no técnico.

Contenidos fundamentales de la asignatura

1. Introducción
2. Preliminares
    1. Conceptos bàsicos
    2. Virtualización (para los labs)
3. Sistemas básicos de seguridad
4. Fallos de programación: stack exploits, etc.
5. Auditoria básica de seguridad
6. Criptografía
    - Criptografía simétrica
        - Cifrado de bloque
        - Cifrado de flujo
    - Funciones Hash
    - Criptografía asimétrica
        - Coneceptos matemáticos
        - El criptosistema RSA
        - Digital signature (DSA)
7. Cortafuegos
    - Filtrado de tráfico de red
    - Diseño de cortafuegos para estaciones, servidores y sistema intermedios
8. Autenticación
    - Gestió de claves
    - Aplicaciones de autenticación
        - kerberos
        - X509
    - Infraestructura de clave pública
    - DNIe
9. Comunicaciones seguras

    - Programación SSL
    - SMIME
    - HTTPS
    - OpenVPN

Ejes metodológicos de la asignatura

Cada uno de los temas que componen la asignatura se presenta en clases magistrales. En función de los contenidos, se propone la resolución de problemas prácticos y/o casos prácticos. Tanto los problemas como los casos prácticos se trabajan en grupo, parcialmente tutorizados en clase y són evaluados.

Plan de desarrollo de la asignatura

Semana 1,2. Temas 1,2
Semana 3,4. Tema 3
Semana 5,6. Temas 4 i 5
Semana 7-10, Tema 6
Semana 11,12, Tema 7
Semana 13,14, Tema 8
Semana 15,16, Tema 9

Sistema de evaluación

La evaluación consistirá en una serie de ejercicios y casos prácticos con la puntuación siguiente:

1. Virtualización (5)
2. Sistemas básicos de seguridad (7 + 7)
3. Fallos de programación: stack exploits, etc. (7)
4. Auditoria básica de seguridad: (8)
5. Criptografía simétrica (3+3+3+3)
6. Funciones Hash (3)
7. Criptografía asimétrica (3+ 3)
8. Cortafuegos (4+4+4)
9. Clave pública con OpenSSL (7.5)
    - DNIe (4.5)
    - PKI (3)
10. Programación con SSL (7.5)
11. SMIME (6)
12. HTTPS (4.5)
13. OpenVPN (3)

De totas estas actividades debe conseguirse, como mínimo, el 50% del total de los puntos para superar la asignatura.

Bibliografía y recursos de información

- Network Security with OpenSSL. Pravir Chandra, Matt Messier, John Viega. Ed. O'Reilly, 2002
- OpenSSL Documents
- Cryptography & Network Security, W. Stallings, 3-Ed, 2003
- Network & Internetwork Security, W. Stallings, 1995
- Advanced Penetration Testing for Highly-Secured Environments. Lee Allen. Packt Publishing. 2012.
- Threat Modeling. Adam Shostack. Wiley. 2014.
- Metasploit Penetration Testing Cookbook. Abhinav Singh. Pack Publishing. 2012.
- Gray Hat Hacking: The Ethical Hackers Handbook. Harper, Harris et al. McGraw-Hill.2011