GUÍA DOCENTE

SEGURIDAD DE APLICACIONES Y COMUNICACIONES

Año académico 2015-16

SEGURIDAD DE APLICACIONES Y COMUNICACIONES 2015-16

Información general de la asignatura

Denominación	Seguridad de Aplicaciones y Comunicaciones
Código	102028
Semestre de impartición	1º Q Evaluación Continuada
Carácter	Obligatoria
Número de créditos ECTS	9
Créditos teóricos	0
Créditos prácticos	0
Departamento/s	DIEI, MATEMATICA
Modalidad	Presencial
Información importante sobre tratamiento de datos	Consulte este enlace para obtener más información.
Idioma/es de impartición	Catalá / Inglés Materiales en Inglés
Grado/Máster	Grado de Ingenieria Informática
Dirección electrónica profesor/a (es/as)	cesar@diei.udl.cat carlesm@diei.udl.cat

SEGURIDAD DE APLICACIONES Y COMUNICACIONES 2015-16

FERNÁNDEZ CAMÓN, CÉSAR
MATEU PIÑOL, CARLES
SEBE FEIXAS, FRANCISCO

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

Estudiar como hacer seguras tanto las infraestructuras (redes y servidores) como las comunicaciones. Asignatura con material en inglés.

Competencias

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.

Contenidos fundamentales de la asignatura

1. Introduction
2. Preliminaries
    1. Introductory concepts
    2. Virtualization (for use in labs)
3. Basic Systems security
4. Programming faults: stack exploits, etc.
5. Basic security auditing
6. Cryptography
    - Symmetric cryptography
        - Block ciphers
        - Stream ciphers
    - Hash functions
    - Asymmetric cryptography
        - Mathematical background
        - The RSA cryptosystem
        - Digital signature (DSA)
7. Firewalls
    - Network traffic filtering
    - Firewall design for workstations, servers and gateways.
8. Authentication
    - Key management

    - Authentication applications
        - kerberos
        - X509
    - Public Key Infrastructure
    - DNIe
9. Comms security
    - SSL programming
    - SMIME
    - HTTPS
    - OpenVPN

Plan de desarrollo de la asignatura

1. Introduction (1t)
2. Preliminaries
    1. Introductory concepts (2t)
    2. Virtualization (for use in labs) (2t, 4l, 1ex)
3. Basic Systems security (6t, 10l, 2ex)
4. Programming faults: stack exploits, etc. (2t, 4l, 1ex)
5. Basic security auditing: (4t, 6l, 1x)
6. Cryptography
    - Symmetric cryptography (6t,4l,4ex)
        - Block ciphers
        - Stream ciphers
    - Hash functions (1t,1l,1ex)
    - Asymmetric cryptography (4t,2l,2ex)
        - Mathematical background
        - The RSA cryptosystem
        - Digital signature (DSA)
7. Firewalls (5t,7l,3ex)
    - Network traffic filtering
    - Firewall design for workstations, servers and gateways
8. Authentication
    - Key management (1t)
    - Authentication applications (2t)
        - kerberos
        - X509
    - Public Key with OpenSSL (2t, 2l, 2ex)
        - PKI (1t, 2l, 1ex)
        - DNIe (2t, 3l, 1ex)
9. Comms security
    - SSL programming (2t, 3l, 2ex)
    - SMIME (1t, 2l, 1ex)
    - HTTPS (1t, 2l, 1ex)
    - OpenVPN (1t, 3l)

Sistema de evaluación

La evaluación consistirá en una serie de ejercicios y problemas (marcados como ex en el plan de desarrollo), que valdrán por:

1. Virtualization (2t, 4l, 1ex-5 punts)
2. Basic Systems security (6t, 10l, 2ex-7 i 7 punts)
3. Programming faults: stack exploits, etc. (2t, 4l, 1ex-7 punts)
4. Basic security auditing: (4t, 6l, 1ex-8 punts)
5. Symmetric cryptography (6t,4l,4ex - 4x3punts)

6. Hash functions (1t,1l,1ex - 3 punts)
7. Asymmetric cryptography (4t,2l,2ex - 2 x 3 punts)
8. Firewalls (5t,7l,3ex - 3 x 4 punts)
9. Public Key with OpenSSL (2t, 2l, 2ex, 7.5pts)
    - DNIe (2t, 3l, 1ex, 4.5pts)
    - PKI (1t, 2l, 1ex, 3pt)
10. SSL programming (2t, 3l, 2ex, 7.5pts)
11. SMIME (1t, 2l, 1ex, 6pts)
12. HTTPS (1t, 2l, 1ex, 4.5pts)
13. OpenVPN (1t, 3l)

De totas estas actividades debe conseguirse, como mínimo, 50 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