UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Ficha del curso: 2015-2016

Grado: GRADO EN INGENIERÍA INFORMÁTICA		**Curso**: Optativas generales 3º y 4º **(** 2C **)**
Asignatura: 803304 - Seguridad en redes **Asignatura en Inglés**: Network security	**Abrev:** SER	6 **ECTS**
Materia: Complementos de computadores		12 **ECTS**
Otras asignaturas en la misma materia: Programación paralela para móviles y multicores		6 ECTS
Módulo: Optativo		
Departamento: Arquitectura de Computadores y Automática	**Coordinador:** Huedo Cuesta, Eduardo	

Descripción de contenidos mínimos:

Redes avanzadas

Programa detallado:

No se oferta para alumnos del Grado en Ingeniería Informática, itinerario Tecnología de la Información.

TEORÍA

Módulo 1. Introducción a la seguridad
- 1.1. Introducción
- 1.2. Vulnerabilidades y amenazas
- 1.3. Anatomía de un ataque
- 1.4. Servicios y mecanismos de seguridad
- 1.5. Aspectos legales y éticos

Módulo 2. Seguridad en las comunicaciones
- 2.1. Introducción a la criptografía
- 2.2. Criptografía de clave secreta
- 2.3. Funciones resumen
- 2.4. Criptografía de clave pública
- 2.5. Certificados digitales y modelos de confianza
- 2.6. Aplicaciones para comunicaciones seguras

Módulo 3. Seguridad en redes
- 3.1. Vulnerabilidades en protocolos de red y ataques
- 3.2. Cortafuegos
- 3.3. Detección de intrusos
- 3.4. Conexiones de red seguras
- 3.5. Seguridad en redes inalámbricas

Módulo 4. Seguridad de servidores de Internet
- 4.1. Seguridad Web
- 4.2. Seguridad del correo electrónico
- 4.3. Seguridad DNS

PRÁCTICAS

Módulo 2. Seguridad en las comunicaciones
- 2.1. Criptografía de clave secreta y funciones resumen (OpenSSL y GnuPG)
- 2.2. Criptografía de clave pública (OpenSSL y GnuPG)
- 2.3. Certificados digitales (OpenSSL y GnuPG)

Módulo 3. Seguridad en redes
- 3.1. Laboratorio virtual para pruebas de seguridad
- 3.2. Ataques a protocolos de red (hping3 y nmap)
- 3.3. Cortafuegos (iptables)
- 3.4. Detección de intrusos (snort)
- 3.5. Conexiones seguras a nivel de red (IPsec)
- 3.6. Conexiones seguras a nivel de transporte (OpenVPN y OpenSSH)

Módulo 4. Seguridad de servidores de Internet
- 4.1. Ataques web (Mutillidae II)
- 4.2. Fortificación de un servidor web (Apache)
- 4.3. Seguridad de e-mail (SPF y DKIM) y DNS (DNSSEC)

Programa detallado en inglés:

THEORY

Module 1. Introduction to security
- 1.1. Introduction
- 1.2. Vulnerabilities and threats

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

1.3. Anatomy of an attack
1.4. Security services and mechanisms
1.5. Ethical and legal aspects
Module 2. Communication security
2.1. Introduction to cryptography
2.2. Secret key cryptography
2.3. Hash functions
2.4. Public key cryptography
2.5. Digital certificates and trust models
2.6. Applications for secure communications
Module 3. Network security
3.1. Network protocol vulnerabilities and attacks
3.2. Firewalls
3.3. Intrusion detection
3.4. Secure network connections
3.5. Wireless network security
Module 4. Internet server security
4.1. Web security
4.2. E-mail security
4.3. DNS security

LABORATORY
Module 2. Communication security
2.1. Secret key cryptography and hash functions (OpenSSL and GnuPG)
2.2. Public key cryptography (OpenSSL and GnuPG)
2.3. Digital certificates (OpenSSL and GnuPG)
Module 3. Network security
3.1. Virtual laboratory for security tests
3.2. Network protocol attacks (hping3 and nmap)
3.3. Firewalls (iptables)
3.4. Intrusion detection (snort)
3.5. Network-level secure connections (IPsec)
3.6. Transport-level secure connections (OpenVPN and OpenSSH)
Module 4. Internet server security
4.1. Web attacks (Mutillidae II)
4.2. Web server hardening (Apache)
4.3. E-mail (SPF and DKIM) and DNS (DNSSEC) security

Competencias de la asignatura:

Generales:

CG16-Conocimiento y aplicación de las características, funcionalidades y estructura de los Sistemas Distribuidos, las Redes de Computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.

Específicas:

No tiene

Básicas y Transversales:

CT1-Capacidad de comunicación oral y escrita, en inglés y español utilizando los medios audiovisuales habituales, y para trabajar en equipos multidisciplinares y en contextos internacionales.

CT2-Capacidad de análisis y síntesis en la resolución de problemas.

CT3-Capacidad para gestionar adecuadamente la información disponible integrando creativamente conocimientos y aplicándolos a la resolución de problemas informáticos utilizando el método científico.

CT5-Capacidad para valorar la repercusión social y medioambiental de las soluciones de la ingeniería, y para perseguir objetivos de calidad en el desarrollo de su actividad profesional.

Resultados de aprendizaje:

No tiene

Evaluación:

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

Todas las pruebas realizadas en cada asignatura serán comunes a todos los grupos de la misma.
Al tener las materias optativas muy diversas características la calificación de las mismas podrá ser muy variada, por lo que los rangos se dejan muy abiertos:
• Exámenes sobre la materia: 0-60%
• Otras actividades: 100-40%

En el apartado "Otras actividades" se podrá valorar la participación activa en el proceso de aprendizaje, la realización de prácticas y ejercicios y la realización de otras actividades dirigidas. La realización de las prácticas de laboratorio y del resto de las actividades evaluables será obligatoria.
Antes del comienzo de cada curso escolar se concretarán en las fichas docentes los porcentajes exactos que se utilizarán durante ese curso para la evaluación de la materia, siendo comunes estos criterios para todos los grupos de una misma asignatura.
La calificación reflejará los resultados de aprendizaje de las diferentes competencias que se adquieren en el módulo o materia.

Evaluación detallada:

Asistencia al laboratorio y realización de prácticas = 40%
Examen final (en aula) = 60%

Exámenes:

☑ En Aula	☐ En Lab
☐ Final Feb	☐ Parcial Feb
☑ Final Jun	☐ Parcial Jun
☑ Final Sep	☐ Sin Examen

Actividades formativas:

Las actividades formativas que se van a realizar para esta materia se dividen en tres grupos:
Actividades presenciales: 30-40% de la dedicación del alumno. Estas actividades podrán incluir:
Clases teóricas magistrales.
Clases de problemas.
Laboratorios.
Seminarios.
Actividades dirigidas: 10-15% de la dedicación del alumno. Estas actividades podrán incluir:
Trabajos dirigidos.
Tutorías dirigidas.
Trabajo personal: 50-55% de la dedicación del alumno. Estas actividades podrán incluir:
Trabajo personal no dirigido: Estudio, preparación de exámenes, realización de ejercicios.
Realización de exámenes.

Actividades docentes:

Reparto de créditos:
Teoria: 3,60
Problemas: 0,00
Laboratorios: 2,40

Otras actividades:
No tiene

Bibliografía:

- E. Cole. Network Security Bible, 2nd Edition. Ed. John Wiley & Sons. 2009
- M. Stewart. Network Security, Firewalls, and VPNs. Ed. Jones & Bartlett Learning. 2010
- J. Vacca. Computer and Information Security Handbook. Ed. Morgan Kaufmann. 2009
- B. Burns y otros. Security Power Tools. Ed. O'Reilly. 2007
- S. MacClure y otros. Hacking exposed 6. Ed. MacGraw Hill. 2009
- R. Johnson and M. Merkow. Security Policies and Implementation Issues. Ed. Jones & Bartlett Learning. 2010

Ficha docente guardada por última vez el **02/07/2015 13:16:00** por el profesor: **Eduardo Huedo Cuesta**

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Fecha: ____ de _____ de _____

Firma del Director del Departamento: