UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Ficha del curso: 2020-2021

Debido la situación especial del curso 2020-2021, para conocer el régimen de presencialidad de las asignaturas se debe comprobar la información que se encuentra publicada en https://informatica.ucm.es/marco-docente-2020-2021

Grado: GRADO EN INGENIERÍA INFORMÁTICA	**Curso**: Optativas itinerario 3º **(** 2C **)**	Idioma: **Español**
Asignatura: 805360 - Redes y seguridad II **Asignatura en Inglés**: Networks Security II	**Abrev:** RS2 **Carácter:** Optativa	4,5 **ECTS**
Materia: Redes y seguridad		9 **ECTS**
Otras asignaturas en la misma materia: Redes y seguridad I		4,5 ECTS
Módulo: Tecnología específica: Tecnologías de la información		
Departamento: Arquitectura de Computadores y Automática	**Coordinador:** Pardines Lence, Inmaculada	

Descripción de contenidos mínimos:

Comunicaciones seguras.
Protección redes y sistemas en red.
Configuración segura de servidores.
Seguridad corporativa: políticas y auditorías de seguridad.

Programa detallado:

==TEORÍA==

Módulo 1. Seguridad en redes
1.1. Vulnerabilidades y técnicas de ataques a protocolos de red
1.2. Protección de redes mediante firewalls
1.3. Conexiones de red seguras
1.4. Sistemas de monitorización y detección de intrusos en red
1.5. Seguridad en redes inalámbricas

Módulo 2. Seguridad en Internet
2.1. Seguridad Web
2.2. Seguridad en e-mail
2.3. Seguridad DNS
2.4. Otras amenazas en Internet

Módulo 3. Gestión de la seguridad
3.1. Legislación sobre seguridad
3.2. Sistema de Gestión de la Seguridad de la Información
3.3. Gestión de incidentes
3.4. Plan de recuperación

==PRÁCTICAS==
0.1 Configuración y conexión de entornos virtuales con varias MV
Módulo 1
1.1 Escaneo y ataques en redes
1.2 Firewalls
1.3 Proxies
1.4 Túneles
1.5 IDS

Módulo 2
2.1 DNSSEC
2.2 Configuración de un Servidor Web seguro (LAMP)
2.3 Pentest Web
2.4 Seguridad e-mail

Programa detallado en inglés:

==THEORY==

Module 1. Network Security

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

1.1 Network protocols' vulnerabilities and attack techniques
1.2 Firewalls
1.3 Secure network connections
1.4 Intrusion Detection/Prevention Systems
1.5 Wireless network security

Module 2. Internet Security
2.1 Web security
2.2 e-mail security
2.3 DNS security
2.4 Other threats in the Internet

Module 3. Security Operation
3.1 Security Legislation
3.2 Information Security Management System
3.3 Incident Management
3.4 Recovery plan

==LABORATORY==

0.1 Introduction to VM configuration and conexion

Module 1
1.1 Network vulnerability scanning and attack techniques
1.2 Proxies
1.3 Tunnels
1.4 IDS

Module 2
2.1 DNSSEC
2.2 LAMP Configuration
2.3 Pentest Web
2.4 e-mail security

Competencias de la asignatura:

Generales:

CG14-Capacidad de conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman.

Específicas:

CE_TI1-Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.

CE_TI4-Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.

CE_TI7-Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

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.

CT4-Capacidad de organización, planificación, ejecución y dirección de recursos humanos.

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.

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

Resultados de aprendizaje:

Analizar vulnerabilidades de sistemas y explotarlos. (CG14, CT2, CT3, CE_TI1, CE_TI4, CE_TI7)

Describir temas relacionados con la asignatura al resto de los compañeros (CG14, CT1, CT4, CT5, CE_TI1, CE_TI4)

Intercambiar información con el resto de compañeros. (CT1, CT4, CT5, CE_TI1, CE_TI4)

Relacionar paradigmas de ataques con su aplicación en diversas tecnologías. (CG14, CT2, CT3, CE_TI1, CE_TI4, CE_TI7)

Resolver retos que requieren conocimientos adquiridos en la asignatura e ingenio. (CG14, CT1, CT2, CT3, CT4, CE_TI1, CE_TI4)

Evaluación:

Todas las pruebas realizadas en cada asignatura serán comunes a todos los grupos de la misma.
La calificación final tendrá en cuenta:
Exámenes sobre la materia: 70-90%
Otras actividades: 10-30%
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:

La asignatura consta de una parte práctica (que no se recupera en la convocatoria extraordinaria) y una parte teórica.

La calificación será:
1) 70% (examen teórico) + 30% (prácticas y otras actividades)
2) 90% (examen teórico-práctico)

El estudiante podrá ser calificado siguiendo la opción marcada como 1 tanto en la convocatoria ordinaria como extraordinaria si ha realizado todas las prácticas y al menos el 66% de las actividades de evaluación continua.

En caso contrario el estudiante será calificado siguiendo la opción 2, este examen se realizará el mismo día y hora que el examen de la opción 1.

La asistencia a la tutorización para la realización de las prácticas durante las 2h reservadas para ello por la asignatura es obligatoria (asistencia virtual/presencial al laboratorio), en caso de que para una práctica particular el estudiante no asista a esta, esa práctica puntuará un 66% de su nota.

Actividades docentes:

Reparto de créditos:
- Teoría: 2,00
- Problemas: 0,00
- Laboratorios: 2,50

Otras actividades:
- Actividades presenciales: enseñanza teórica y realización de prácticas.
- Trabajo personal: realización de las prácticas, preparación del examen, participación activa en clase.
- Participación activa en clase: propuesta de mejoras (teoría y prácticas), propuesta y discusión de temas relacionados con la temática de la asignatura, propuesta y defensa en el aula de un tema consensuado con el profesor.

Bibliografía:

- E. Cole. Network Security Bible, 2nd Edition. Ed. John Wiley & Sons. 2009
- 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
- S. Harris, F. Maymí, Mc Graw Hill, All in one CISSP, exam guide, 7ª edición 2016
- William Stallings Network Security Essentials: Applications and Standards, Prentice Hall, 2013
- J. Michael Stewart, Jones & Bartlett Learning, Network Security, Firewalls, and VPNs, 2014
- Ruby B. Lee, Security Basics for Computer Architects, Synthesis Lectures on Computer Architecture, 2013

Ficha docente guardada por última vez el **21/07/2020 13:07:00** por el departamento: **Arquitectura de Computadores y Automática**

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Fecha: ____ de _____ de _____

Firma del Director del Departamento: