UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. DATOS GENERALES

Asignatura: SEGURIDAD EN REDES
Código: 42340
Tipología: OBLIGATORIA
Créditos ECTS: 6
Grado: 346 - GRADO EN INGENIERÍA INFORMÁTICA (AB)
Curso académico: 2019-20
Centro: 604 - E.S. DE INGENIERIA INFORMATICA ALBACETE
Grupo(s): 16
Curso: 4
Duración: Primer cuatrimestre
Lengua principal de impartición: Español
Segunda lengua: Inglés
Uso docente de otras lenguas:
English Friendly: S
Página web: https://esiiab.uclm.es/asig.php?codasig=42340&curso=2018-19
Bilingüe: N

Profesor: **JOSE LUIS MARTINEZ MARTINEZ** - Grupo(s): **16**

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
ESII-1.C.11	SISTEMAS INFORMÁTICOS	2294	joseluis.martinez@uclm.es	Publicada en la página de la ESII. Se atenderá cualquier día y hora previa cita a través del mail

2. REQUISITOS PREVIOS

Asignatura obligatoria para la Materia de Tecnología Específica de Ingeniería de Computadores, es aconsejable haber cursado los módulos de Formación Básica y el módulo Común a la Rama de Informática (Módulos I y II). Se recomienda por tanto tener claros los conceptos básicos de redes de interconexión y configuración de dispositivos en red, y conceptos de programación y sistemas operativos.

3. JUSTIFICACIÓN EN EL PLAN DE ESTUDIOS, RELACIÓN CON OTRAS ASIGNATURAS Y CON LA PROFESIÓN

Esta asignatura forma parte de la materia Tecnología Específica de Ingeniería de Computadores, dentro de la intensificación Ingeniería de Computadores. Es una materia obligatoria para obtener la mención correspondiente a la citada intensificación.

Ayuda a alcanzar una de las capacidades que deben tener los graduados en Ingeniería Informática de la UCLM, en concreto, la capacidad [IC6]: Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Los contenidos tratados en esta asignatura están íntimamente relacionados a los de otras asignaturas impartidas en el plan, como son Redes de Computadores I, Redes de Computadores II, Diseño y Gestión de Redes, Dispositivos y Redes Inalámbricos, Criptografía, Auditoría en Sistemas de Información, Sistemas Operativos I y II.

4. COMPETENCIAS DE LA TITULACIÓN QUE LA ASIGNATURA CONTRIBUYE A ALCANZAR

Competencias propias de la asignatura

Código	Descripción
IC6	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
INS1	Capacidad de análisis, síntesis y evaluación.
INS2	Capacidad de organización y planificación.
INS4	Capacidad de resolución de problemas aplicando técnicas de ingeniería.
PER2	Capacidad de trabajo en equipo interdisciplinar.
SIS1	Razonamiento crítico.
SIS3	Aprendizaje autónomo.
SIS5	Creatividad.

5. OBJETIVOS O RESULTADOS DE APRENDIZAJE ESPERADOS

Resultados de aprendizaje propios de la asignatura

Descripción

Diseñar, implantar y configurar el acceso remoto seguro.

Explicar y aplicar los principios de seguridad necesarios para proteger a una red y a los dispositivos en ella incluidos.

6. TEMARIO

Tema 1: Introduction

- **Tema 1.1** Presentation
- **Tema 1.2** Introduction to Security

Tema 2: Ethical Hacking

- **Tema 2.1** Footprinting and Open Source Intelligenca
- **Tema 2.2** Scaning and Enumeration
- **Tema 2.3** NavajaNegra Conference
- **Tema 2.4** Attacks to credentials and Social Engeniering
- **Tema 2.5** Attacks to Networks

Tema 2.6 Exploiting
Tema 2.7 PostExploiting
Tema 2.8 Python for pentester
Tema 3: Reverse Enggeniering
Tema 3.1 Introduction to reversing
Tema 3.2 Cracking
Tema 3.3 Advanced Exploiting
Tema 3.4 Malware Analysis

7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

Actividad formativa	Metodología	Competencias relacionadas (para títulos anteriores a RD 822/2021)	ECTS	Horas	Ev	Ob	Rec	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Combinación de métodos	IC6 INS1 SIS1	1.04	26	S	N	S	Presentación de los temas de la asignatura en clase
Enseñanza presencial (Prácticas) [PRESENCIAL]	Prácticas	IC6 SIS1	1.2	30	S	N	S	Desarrollo de las prácticas de laboratorio
Presentación de trabajos o temas [PRESENCIAL]	Trabajo en grupo	IC6 INS1 INS2 INS4 PER2 SIS1 SIS3 SIS5	0.12	3	S	N	S	Exposición pública en clase del trabajo de la asignatura
Prueba final [PRESENCIAL]	Resolución de ejercicios y problemas	IC6 INS1 SIS1 SIS5	0.2	5	S	S	S	Examen Final Teórico y Práctico
Pruebas on-line [AUTÓNOMA]	Pruebas de evaluación	IC6 SIS1 SIS5	0.16	4	S	N	S	Diferentes tests realizados a lo largo del curso tanto teóricos como prácticos para llevar a cabo el modo de evaluación mediante evaluación continua
Elaboración de informes o trabajos [AUTÓNOMA]	Autoaprendizaje	IC6 INS1 INS2 INS4 PER2 SIS1 SIS3 SIS5	0.8	20	S	N	S	Realización de un trabajo a lo largo del curso relacionados con la asignatura y su posterior exposición en clase
Estudio o preparación de pruebas [AUTÓNOMA]	Trabajo autónomo	INS1 INS2 INS4	2.48	62	S	N	S	Trabajo en casa para la preparación de los tests de prácticas y teoría y del examen final (teórico-práctico)
		Total:	**6**	**150**				
		Créditos totales de trabajo presencial: 2.56						**Horas totales de trabajo presencial: 64**
		Créditos totales de trabajo autónomo: 3.44						**Horas totales de trabajo autónomo: 86**

Ev: Actividad formativa evaluable
Ob: Actividad formativa de superación obligatoria
Rec: Actividad formativa recuperable

8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

	Valoraciones		
Sistema de evaluación	**Estudiante presencial**	**Estud. semipres.**	**Descripción**
Prueba final	25.00%	0.00%	Prueba final correspondiente a la parte de teoría. Corresponde con la categoría "ESC" de la memoria de grado.
Prueba final	25.00%	0.00%	Resolución de un problema en el laboratorio, derivado de los contenidos de prácticas [Además se podrán consultar cualquier material durante el examen] que corresponde con la categoría "INF" de la memoria de grado.
Pruebas de progreso	50.00%	0.00%	Se realizarán mecanismos de evaluación para realizar una evaluación contínua del contenido teórico y práctico de la asignatura. Corresponde con la categoría "ESC", "LAB" y "PRES" de la memoria de grado.
Total:	**100.00%**	**0.00%**	

Criterios de evaluación de la convocatoria ordinaria:
[MODALIDAD CON EVALUACIÓN CONTÍNUA]
-Teoría:
- Examen Final Teórico: 25% (Nota mínima: 4 puntos. Compensable con la evaluación contínua)
-Prácticas:
- Examen de Final Práctico de Laboratorio: 25% (Nota mínima: 4 puntos. Compensable con la evaluación contínua)
-Evaluación Contínua:
- Test Evaluables: 50% Se realizarán 5 mecanismos de evalución (10% cadad uno) a lo largo de la asignatura.

[MODALIDAD SIN EVALUACIÓN CONTÍNUA]
-Teoría:
- Examen Final: 50% (Nota mínima: 4 puntos. Compensable con la parte de prácticas)
-Prácticas:
- Examen Final de Prácticas: 50% (Nota mínima: 4 puntos. Compensable con la parte de teoría)

En ambas modalidades se guarda cada parte para la convocatoria extraordinaria si se supera el 5

El alumno que no supere todas las pruebas mínimas exigidas (nota mínima de 4 tanto en el examen de teoría Y prácticas) en la asignatura aparecerá como suspenso y tendrá una nota final correspondiente a la nota media entre el examen de teoría y prácticas. En caso de que la media de aprobado, tendrá una nota de suspenso, 4.

Particularidades de la convocatoria extraordinaria:

En la convocatoria extraordinaria solo se podrá recuperar el examen final de teoría y el caso práctico en el laboratorio, las notas de la evaluación contínua se mantienen de la ordinaria. Si el alumno lo desea, puede presentarse según el formato CON O SIN MODALIDAD EVALUACIÓN CONTÍNUA, es decir, con o sin tener en cuenta los resultados de la evaluación contínua

Particularidades de la convocatoria especial de finalización:

Las mismas que la extraordinaria

9. SECUENCIA DE TRABAJO, CALENDARIO, HITOS IMPORTANTES E INVERSIÓN TEMPORAL

No asignables a temas

Horas	Suma horas
Presentación de trabajos o temas [PRESENCIAL][Trabajo en grupo]	3
Prueba final [PRESENCIAL][Resolución de ejercicios y problemas]	5
Pruebas on-line [AUTÓNOMA][Pruebas de evaluación]	4
Elaboración de informes o trabajos [AUTÓNOMA][Autoaprendizaje]	20

Comentarios generales sobre la planificación: Esta planificación es ORIENTATIVA, pudiendo variar a lo largo del periodo lectivo en función de las necesidades docentes, festividades, o por cualquier otra causa imprevista. La planificación semanal de la asignatura podrá encontrarse de forma detallada y actualizada en la plataforma Campus Virtual (Moodle). Además, las actividades de evaluación o recuperación de clases podrían planificarse, excepcionalmente, en horario de tarde

Tema 1 (de 3): Introduction

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	4
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	2

Periodo temporal: semana 1

Tema 2 (de 3): Ethical Hacking

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	12
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	20
Elaboración de informes o trabajos [AUTÓNOMA][Autoaprendizaje]	32
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	8

Periodo temporal: semana 2-9

Tema 3 (de 3): Reverse Enggeniering

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	6
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	10
Elaboración de informes o trabajos [AUTÓNOMA][Autoaprendizaje]	20
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	4

Periodo temporal: semana 10-14

Actividad global

Actividades formativas	Suma horas
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	30
Presentación de trabajos o temas [PRESENCIAL][Trabajo en grupo]	3
Prueba final [PRESENCIAL][Resolución de ejercicios y problemas]	5
Pruebas on-line [AUTÓNOMA][Pruebas de evaluación]	4
Elaboración de informes o trabajos [AUTÓNOMA][Autoaprendizaje]	72
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	14
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	22
Total horas:	150

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	Título/Enlace Web	Editorial	Población	ISBN	Año	Descripción
Catherine Paquet	Implementing Cisco IOS Network Security (IINS): (CCNA Security exam 640-553) (Authorized Self-Study Guide)	Cisco Press			2009	
Cisco Systems	Fundamentos de seguridad de redes : Especialista en Firewall Cisco / Cisco System ; traducción, José Manuel Díaz Madrid	Pearson Education			2008	
Michael Walkings, Kevin Wallace	CCNA Security Official Exam Certification Guide	Cisco Press			2008	
William Stallings	Fundamentos de seguridad en redes : aplicaciones y estándares	Prentice Hall			2003	
varios	Colección Pack Completa http://0xword.com/es/	0xword				Colección de varios ejemplares