1. Identificación

1.1. De la Asignatura

Curso Académico	2022/2023
Titulación	MÁSTER UNIVERSITARIO EN NUEVAS TECNOLOGÍAS EN INFORMÁTICA
Nombre de la Asignatura	SEGURIDAD Y CONFIANZA EN SISTEMAS DISTRIBUIDOS
Código	4906
Curso	PRIMERO
Carácter	OPTATIVA
N.º Grupos	1
Créditos ECTS	6
Estimación del volumen de trabajo del alumno	150
Organización Temporal/Temporalidad	Cuatrimestre
Idiomas en que se imparte	INGLÉS
Tipo de Enseñanza	Presencial

1.2. Del profesorado: Equipo Docente

Coordinación de la asignatura ANTONIO RUIZ MARTINEZ Grupo de Docencia: 1	Área/Departamento	INGENIERÍA TELEMÁTICA/INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES
	Categoría	PROFESORES TITULARES DE UNIVERSIDAD
	Correo Electrónico / Página web / Tutoría electrónica	arm@um.es https://webs.um.es/arm/ Tutoría Electrónica: SÍ

Coordinación de los grupos:1	Teléfono, Horario y Lugar de atención al alumnado	Duración	Día	Horario	Lugar
		Primer Cuatrimestre	Martes	12:00- 13:30	(Sin Extensión), Facultad de Informática B1.1.044
		Primer Cuatrimestre	Viernes	16:00- 17:30	(Sin Extensión), Facultad de Informática B1.1.044
		Segundo Cuatrimestre	Jueves	17:00- 19:00	(Sin Extensión), Facultad de Informática B1.1.044
		Segundo Cuatrimestre	Viernes	12:00- 13:30	(Sin Extensión), Facultad de Informática B1.1.044
FELIX GOMEZ MARMOL Grupo de Docencia: 1	Área/Departamento	INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	Categoría	PROFESORES TITULARES DE UNIVERSIDAD			
	Correo Electrónico / Página web / Tutoría electrónica	felixgm@um.es https://webs.um.es/felixgm/ Tutoría Electrónica: SÍ			

	Teléfono, Horario y Lugar de atención al alumnado	Duración	Día	Horario	Lugar
		Primer Cuatrimestre	Lunes	15:00- 18:00	868889782, Facultad de Informática B1.1.034
		Segundo Cuatrimestre	Martes	15:30- 18:30	868889782, Facultad de Informática B1.1.034
PANTALEONE NESPOLI Grupo: 1	Categoría	CONTRATO DE ACCESO AL SECTI			
	Correo Electrónico / Página web / Tutoría electrónica	pantaleone.nespoli@um.es https://webs.um.es/pantaleone.nespoli Tutoría Electrónica: SÍ			
	Teléfono, Horario y Lugar de atención al alumnado				

2. Presentación

Esta asignatura centra su docencia en temas investigación e innovación relacionados con la seguridad y la confianza en sistemas distribuidos de comunicaciones. En particular, se centra en la descripción de los principales retos de investigación en honeypots, SIEM y OSINT. De igual manera, la asignatura aborda los principales aspectos relacionados con la privacidad y el anonimato en los sistemas de comunicaciones actuales.

3. Condiciones de acceso a la asignatura

3.1 Incompatibilidades

No consta

3.2 Recomendaciones

Es muy recomendable haber cursado antes la asignatura "Tecnologías Básicas de Comunicaciones" del primer cuatrimestre.

Se requieren los principales conocimientos de redes,seguridad y criptografía impartidos en las asignaturas de "Arquitectura de Redes", "Servicios Telemáticos" y "Seguridad" del Grado en Ingeniería Informática de la Universidad de Murcia.

4. Competencias

4.1 Competencias Básicas

No disponible

4.2 Competencias de la titulación

· CGT1. Capacidad para comprender y aplicar métodos y técnicas de investigación en el ámbito de la Ingeniería Informática.
· CET3. Capacidad para integrar los conocimientos adquiridos y aplicarlos al resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares

4.3 Competencias transversales y de materia

· Competencia 1. CRT3 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información

5. Contenidos

TEMA 1. Introducción a Seguridad y Confianza en Sistemas Distribuidos

TEMA 2. Honeypots

TEMA 3. OSINT

TEMA 4. SIEM

TEMA 5. Privacidad y anonimato: identificación de riesgos y soluciones asociadas

PRÁCTICAS

Práctica 1. Honeypots: Relacionada con los contenidos Tema 2

Práctica 2. OSINT: Relacionada con los contenidos Tema 3

Práctica 3. SIEM: Relacionada con los contenidos Tema 4

Práctica 4. Privacidad y anonimato: Relacionada con los contenidos Tema 5

6. Metodología Docente

Actividad Formativa	Metodología	Horas Presenciales	Trabajo Autónomo	Volumen de trabajo
A1-Clase magistral	Actividades con grupo grande de alumnos/as entre las que se encuentran la presentación en el aula de los conceptos propios de la materia mediante metodología expositiva con lecciones magistrales participativas y medios audiovisuales y/o metodologías activas como aula invertida. También se contemplan en este grupo las actividades de evaluación teórico-prácticas.	19,2	0	19.2
A2-Seminarios	Actividades con grupo mediano en el aula de resolución de problemas, seminarios, charlas, ejercicios basados en el aprendizaje orientado a proyectos, estudios de casos, exposición y discusión de trabajos relativas al seguimiento individual y/o grupal de adquisición de las competencias.	6	0	6
A3-Laboratorios	Actividades con grupo pequeño en el laboratorio relacionadas con la componente práctica de las asignaturas, desarrollo de trabajos con equipo técnico especializado, desarrollo de programas, etc.	18	0	18

Actividad Formativa	Metodología	Horas Presenciales	Trabajo Autónomo	Volumen de trabajo
A4-Tutorías	Tutorías individualizadas o en grupo muy pequeño orientadas a la dirección, supervisión y asesoría por parte de un profesor de la asignatura que de forma periódica constate y redirija el trabajo del alumno/a hacia la consecución de los objetivo marcados.	4,8	0	4.8
A5-Trabajo autónomo	Estudio y trabajo autónomo orientado a la asimilación de contenidos, realización de problemas, ejercicios o redacción de informes técnicos o memorias descriptivas, desarrollo de proyectos o prácticas individuales o en grupo, preparación de exámenes, presentaciones y defensa de trabajos.		102	102
	Total	48	102	150

7. Horario de la asignatura

https://www.um.es/web/estudios/grados/informatica/horarios-examenes

8. Sistema de Evaluación

Métodos / Instrumentos	Examen teórico-práctico: En este instrumento incluimos desde el tradicional examen escrito o tipo test hasta los exámenes basados en resolución de problemas, pasando por los de tipo mixto que incluyen cuestiones cortas o de desarrollo teórico junto con pequeños problemas. También se incluye aquí la consideración de la participación activa del alumno en clase, la entrega de ejercicios o realización de pequeños trabajos escritos y presentaciones.
Criterios de Valoración	Examen escrito en inglés con preguntas cortas y largas de desarrollo relacionadas con los temas tratados tanto en las sesiones de teoría como en las sesiones prácticas. Es necesario superar esta parte con, al menos, un 5 para realizar el cálculo de la nota final del curso.
Ponderación	50
Métodos / Instrumentos	Informe técnico: En este instrumento incluimos los resultados de actividades prácticas, o de laboratorio junto con sus memorias descriptivas, los resúmenes del estado del arte o memorias de investigación sobre temas concretos. Y la posibilidad de realizar entrevistas personales o presentaciones de los trabajos realizados también entran en esta categoría.
Criterios de Valoración	Trabajos prácticos relacionados con cada una de las prácticas de la asignatura. La realización de cada una de las prácticas implicará, por un lado, la realización de un informe técnico donde se explicarán y justificarán los principales aspectos desarrollados en la práctica y, por otro lado, se tendrá que realizar una defensa pública de dicho informe. Es necesario superar esta parte con, al menos, un 5 para realizar el cálculo de la nota final del curso.
Ponderación	50

Fechas de exámenes

https://www.um.es/web/estudios/grados/informatica/horarios-examenes

9. Resultados del Aprendizaje

- Identificar vulnerabilidades y posibles escenarios de ataques.
- Conocer el despliegue de sistemas de detección y prevención de intrusos.
- Conocer los modelos y paradigmas de gestión de seguridad en las comunicaciones.

- Conocer y aplicar los principales aspectos relacionados OSINT y SIEM.
- Conocer las principales técnicas de gestión de privacidad y anonimato.
- Distinguir entre los distintos mecanismos de rastreo existentes.
- Usar distintas soluciones contra el rastreo y protocolos de comunicaciones anónimas.
- Evaluar distintos escenarios de privacidad identificando riesgos y proponiendo soluciones.

10. Bibliografía

Bibliografía Complementaria

C.P. Pfleeger, S.L. Pfleeger, Security in Computing, 4th Edition, 4th ed., Prentice Hall, 2006.

David G. Birch. Digital Identity Management. Gower Publishing, Ltd. 2007.

J. Ren, J. Wu, Survey on anonymous communications in computer networks, Comput. Commun. 33 (2010) 420-431.

William Stallings. Network Security Essentials. Prentice Hall. Segunda edición. 2002.

M. Hansen, A. Schwartz, A. Cooper, Privacy and Identity Management, IEEE Security and Privacy. 6 (2008) 38-45.

P. Guarda, N. Zannone, Towards the development of privacy-aware systems, Inf. Softw. Technol. 51 (2009) 337-350.

Sean Convery. Network Security Architectures. Cisco Press. 2004.

J. Rittinghouse, J. Ransome. Cloud Computing: Implementation, Management, and Security. CRC Press. 2009.

Stallings, William., Network security essentials : applications and standards /(2007) ,Pearson Education,

Stallings, William., Network security essentials : applications and standards /(2003) ,Pearson Education,

11. Observaciones y recomendaciones

Si el estudiante NO ha aportado TODAS las evidencias de evaluación (tareas, exámenes, etc) que permitan una calificación global de la asignatura, se consignará en el acta la calificación de "No Presentado".

Es necesario obtener una nota superior al 5 sobre 10 en cada una de las partes evaluadas (teoría y prácticas), para poder aprobar la asignatura

No se guardan partes aprobadas para cursos próximos.

Las entregas de prácticas que se soliciten se realizarán a través de las tareas abiertas en Aula Virtual a tal efecto y dentro del plazo estipulado. Las entregas realizadas por cualquier otro medio o fuera de plazo no serán aceptadas.

Necesidades educativas especiales. Aquellos estudiantes con discapacidad o necesidades educativas especiales pueden dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV; http://www.um.es/adyv/) para recibir la orientación o asesoramiento oportunos para un mejor aprovechamiento de su proceso formativo. De igual forma podrán solicitar la puesta en marcha de las adaptaciones curriculares individualizadas de contenidos, metodología y evaluación necesarias que garanticen la igualdad de oportunidades en su desarrollo académico. El tratamiento de la información sobre este alumnado es de estricta confidencialidad, conforme a lo dispuesto en los reglamentos y normativa vigente actual.

Las competencias básicas que cubre la asignatura son:

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.