Guía docente

Identificación de la asignatura

Asignatura / Grupo	22383 - Técnicas y Aplicaciones de Seguridad en Redes Telemáticas / 4
Titulación	Grado en Ingeniería Telemática - Cuarto curso
Créditos	6
Período de impartición	Primer semestre
Idioma de impartición	Castellano

Profesores

	Horario de atención a los alumnos					
Profesor/a	**Hora de inicio**	**Hora de fin**	**Día**	**Fecha inicial**	**Fecha final**	**Despacho / Edificio**
María Francisca Hinarejos Campos *(Responsable)* xisca.hinarejos@uib.es	09:30	11:00	Jueves	01/02/2019	01/07/2019	D-136
	09:30	11:00	Miércoles	01/02/2019	01/07/2019	D-136

Contextualización

Técnicas y Aplicaciones de Seguridad en Redes Telemáticas es una asignatura que forma parte del módulo optativo del plan de estudios del Grado en Ingeniería Telemática.

La asignatura está destinada a ampliar y profundizar en algunos de los conocimientos adquiridos en la asignatura Seguridad en Redes impartida en tercer curso del grado. Además se introducirán nuevos conocimientos, intentando introducirlos desde una visión práctica, pero sin dejar de lado su fundamentación teórica.

A grandes rasgos se explicarán los problemas de seguridad tanto en redes cableadas como en redes inalámbricas. También se adquirirán conocimientos del funcionamiento y acceso a sevidores seguros, del control de acceso a redes (firewalls, redes privadas virtuales, etc), de la descarga e instalación segura de aplicaciones móviles, de vulnerabilidates (identificación y explotación), de los test de penetración, etc.

Requisitos

Esenciales

Es necesario que se haya cursado la asignatura Seguridad en Redes Telemáticas de tercer curso de grado. Este hecho implica haber cursado las asignaturas que son requisito de la asignatura Seguridad en Redes Telemáticas.

Recomendables

Fecha de publicación: 24/07/2018

Competencias

Específicas

* CC2: Capacidad de utilizar aplicaciones de comunicación e informáticas (ofimáticas, bases de datos, cálculo avanzado, gestión de proyectos, visualización, etc.) para apoyar el desarrollo y explotación de redes, servicios y aplicaciones de telecomunicación y electrónica .
* CC13: Capacidad de diferenciar los conceptos de redes de acceso y transporte, redes de conmutación de circuitos y de paquetes, redes fijas y móviles, así como los sistemas y aplicaciones de red distribuidos, servicios de voz, datos, audio, video y servicios interactivos y multimedia. .

Genéricas

* CG1: Razonamiento crítico: capacidad para analizar y valorar diferentes alternativas .
* CG2: Resolución de problemas: capacidad para encontrar las soluciones óptimas a problemas y proyectos complejos .
* CG4: Habilidad de adaptación a la rápida evolución de las tecnologías y los mercados de las TIC .

Transversales

* CT2: Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos. .
* CT3: Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis. .
* CT7: Capacidad de programación de servicios y aplicaciones telemáticas, en red y distribuidas .

Básicas

* Se pueden consultar las competencias básicas que el estudiante tiene que haber adquirido al finalizar el grado en la siguiente dirección: http://estudis.uib.cat/es/grau/comp_basiques/

Contenidos

Contenidos temáticos

Tema 1. Introducción
* Objetivos
* Revisión de conceptos de seguridad básica
* Tipos de redes y sus problemas de seguridad
* Ciclo de un test de penetración

Tema 2. Infraestructura de Clave Pública
* ¿Por qué certificados digitales? Del e-DNI a las apps móviles
* Gestión de certificados
* Acceso web seguro: Configuración servidor web seguro
* Análisis de aplicaciones móviles

Fecha de publicación: 24/07/2018

Tema 3. Seguridad perimetral en redes cableadas
* Problemas de seguridad
* Acceso remoto seguro: Configuración de SSH
* Acceso seguro corporativo: Firewalls, VPN, etc.

Tema 4. Seguridad en redes inalámbricas
* Problemas de seguridad
* ¿Es mi red wifi segura?. Seguridad en 802.11: Una visión general
* Configuración segura wifi empresarial

Tema 5. Proyecto de seguridad
* Desarrollo de un proyecto de seguridad relacionado con alguno de los temas dados o con otros temas propuestos (ataques man-in-the-middle, sql injection, information gathering, vulnerabilities, etc.)

Metodología docente

Actividades de trabajo presencial (2,4 créditos, 60 horas)

Modalidad	Nombre	Tip. agr.	Descripción	Horas
Clases teóricas	Clases Magistrales	Grupo grande (G)	Explicación de los conceptos teóricos del temario de la asignatura.	10
Clases prácticas	Prácticas	Grupo mediano (M)	Las prácticas de laboratorio sirven tanto para poner en práctica algunos de los conocimientos teóricos explicados en las clases magistrales como para adquirir nuevos conocimientos. Estas prácticas se realizarán en grupos pequeños de alumnos.	30
Clases de laboratorio	Proyecto	Grupo pequeño (P)	Durante la última parte del curso, se realizará un proyecto (individual o en grupo) sobre alguno de los temas del temario, o de otros temas que se le ofrecerán a los alumnos.	20
Evaluación	Actitud	Grupo grande (G)	La actitud del alumno será valorada a lo largo de todo el semestre.	0

Al inicio del semestre estará a disposición de los estudiantes el cronograma de la asignatura a través de la plataforma UIBdigital. Este cronograma incluirá al menos las fechas en las que se realizarán las pruebas de evaluación continua y las fechas de entrega de los trabajos. Asimismo, el profesor o la profesora informará a los estudiantes si el plan de trabajo de la asignatura se realizará a través del cronograma o mediante otra vía, incluida la plataforma Aula Digital.

Actividades de trabajo no presencial (3,6 créditos, 90 horas)

Modalidad	Nombre	Descripción	Horas
Estudio y trabajo autónomo individual o en grupo	Estudio individual o en grupo	El estudio individual (o en grupo) le servirá al alumno tanto para obtener o consolidar los contenidos teóricos de la asignatura, como para preparar o finalitzar las sesiones de prácticas de laboratorio.	90

Fecha de publicación: 24/07/2018

Riesgos específicos y medidas de protección

Las actividades de aprendizaje de esta asignatura no conllevan riesgos específicos para la seguridad y salud de los alumnos y, por tanto, no es necesario adoptar medidas de protección especiales.

Evaluación del aprendizaje del estudiante

El alumno obtendrá una calificación numérica entre 0 y 10 en cada una de las actividades evaluativas, la cual será ponderada según su peso a fin de obtener la calificación final de la asignatura. Para poder superar la asignatura el alumno ha de obtener un mínimo de 5 puntos sobre 10 mediante la suma ponderada de todas las actividades realizadas.

Durante el semestre se realizarán evaluaciones sobre las prácticas de laboratorio y del proyecto, consistentes en la entrega de memorias de prácticas y/o en la verificación del correcto funcionamiento de la instalación y configuración llevada a cabo por cada alumno. La evaluación ordinaria se realiza sobre la evaluación continua de las prácticas y del proyecto. Las prácticas y el proyecto son recuperables durante el periodo de recuperación, mediante la realización de un examen sobre los conocimientos adquiridos durante el curso.

Convocatoria Anticipada

En esta asignatura no se permite la convocatoria anticipada

Fraude en elementos de evaluación

De acuerdo con el artículo 33 del Reglamento académico, "con independencia del procedimiento disciplinario que se pueda seguir contra el estudiante infractor, la realización demostradamente fraudulenta de alguno de los elementos de evaluación incluidos en guías docentes de las asignaturas comportará, a criterio del profesor, una minusvaloración en su calificación que puede suponer la calificación de «suspenso 0» en la evaluación anual de la asignatura".

Prácticas

Modalidad	Clases prácticas
Técnica	Informes o memorias de prácticas **(recuperable)**
Descripción	Las prácticas de laboratorio sirven tanto para poner en práctica algunos de los conocimientos teóricos explicados en las clases magistrales como para adquirir nuevos conocimientos. Estas prácticas se realizarán en grupos pequeños de alumnos.
Criterios de evaluación	Participación dentro del grupo de prácticas tanto en su preparación como en la resolución de las mismas. Exactitud de los resultados obtenidos y razonamiento de los mismos. Claridad e inteligibilidad de los informes y de las configuraciones realizadas. Se trabajarán las competencias CG2, CT2, CT3, CT7, CC2 y CC13

Porcentaje de la calificación final: 60%

Fecha de publicación: 24/07/2018

Proyecto

Modalidad	Clases de laboratorio
Técnica	Pruebas de ejecución de tareas reales o simuladas **(recuperable)**
Descripción	Durante la última parte del curso, se realizará un proyecto (individual o en grupo) sobre alguno de los temas del temario, o de otros temas que se le ofrecerán a los alumnos.
Criterios de evaluación	Participación durante el desarrollo del proyecto, tanto en su diseño como en su ejecución. Exactitud del resultado obtenido y justificación del mismo. Claridad e inteligibilidad de los informes y de las configuraciones realizadas (si fueran necesarias). Se trabajarán las competencias CG1, CG2, CG4, CT2, CT7, CC2 y CC13

Porcentaje de la calificación final: 30%

Actitud

Modalidad	Evaluación
Técnica	Escalas de actitudes **(no recuperable)**
Descripción	La actitud del alumno será valorada a lo largo de todo el semestre.
Criterios de evaluación	Actitud del alumno tanto individual como dentro del grupo del laboratorio. Se evaluarán las competencias CG1, CG2, CG4, CT2, CT3, CT7, CC2 y CC13

Porcentaje de la calificación final: 10%

Recursos, bibliografía y documentación complementaria

Bibliografía básica

* Jon Edney, William A. Arbaugh. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. ISBN-13: 978-0321136206
* ITU, Information technology “Open Systems Interconnection“ The Directory: Public-key and attribute certificate frameworks Technical Corrigendum 2, Series x: Data networks, open system communications and security directory, ITU-T Recommendation X.509 (Nov 2008)
* Eric F. Crist and Jan Just Keijser. Mastering OpenVPN. Packt Publishing (August 2015). ISBN: 9781783553136
* Recursos en línea que se porporcionarán junto con el material de cada tema a lo largo del curso.

Bibliografía complementaria

La bibliografía recomendada en la asignatura de Seguridad en Redes.

Otros recursos

A través de la página web de la asignatura en Campus Extens, se podrán obtener otros recursos, como enlaces a páginas web con información complementaria, material para las prácticas de laboratorio, etc.

Fecha de publicación: 24/07/2018