Universidad Rey Juan Carlos

GUÍA DOCENTE

PENTESTING

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2024-25

I.-Identificación de la Asignatura	
Tipo	OBLIGATORIA
Período de impartición	4 curso, 1Q semestre
Nº de créditos	3
Idioma en el que se imparte	Castellano

II.-Presentación

Esta asignatura pretende ser un curso introductorio a los test de penetración. Los test de penetración, o pentesting, consisten en simular ataques reales para evaluar el riesgo asociado a potenciales brechas de seguridad. El objetivo es descubrir y explotar vulnerabilidades para evaluar a qué activos podría ganar acceso un posible atacante malicioso. Se estudiarán todas las fases que tiene un pentesting, desde la fase de reconocimiento hasta la fase de escalada de privilegios y mantenimiento del acceso.
Esta asignatura se imparte en el primer cuatrimestre del cuarto curso de la titulación. Para la realización de esta asignatura serán necesarios los conocimientos de asignaturas previas como son técnicas de hacking, desarrollo web seguro, metodologías de desarrollo seguro, programación, redes, administración de sistemas, etc.

III.-Competencias

Competencias Generales

CG6. Capacidad para conocer, comprender y aplicar la legislación y código ético necesario para la labor profesional en el sector de la ciberseguridad.
CG7. Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.

Competencias Específicas

CE20. Analizar las etapas o pasos que los atacantes siguen para construir sus ataques de manera que se puedan comprender los patrones de ataque más graves e importantes y llevarlos a cabo en entornos de seguridad ofensiva.
CE21. Analizar y cuantificar el riesgo que corre un determinado activo, evaluar sus vulnerabilidades e identificar los potenciales impactos de un ciberataque, calibrando su criticidad.
CE34. Escoger el tipo de auditoría más adecuado para cada contexto, ser capaz de elegir o desarrollar las herramientas más adecuadas para llevarla a cabo y analizar los resultados obteniendo conclusiones relevantes.

IV.-Contenido

IV.A.-Temario de la asignatura

Tema	Descripción
Tema 1. Introducción a los test de penetración.	Utilidad y necesidad de los test de penetración, en qué consisten y etapas de un test de penetración. Comunicación con el cliente, establecer el alcance, confidencialidad (NDA y contratos), formato de los informes. Herramientas para pentesters.
Tema 2. Pentesting en entornos Linux.	Herramientas, desarrollo de exploits. Particularidades de los servicios web basados en Linux (Apache, Nginx, etc.) .
Tema 3. Pentesting en entornos Windows.	Herramientas, desarrollo de exploits. Particularidades de los servicios web basados en Windows (IIS, Active Directory, etc.).
Tema 4. Pentesting en entornos móviles.	Herramientas de depuración e Ingeniería inversa.

IV.B.-Actividades formativas

Tipo	Descripción
Prácticas	Práctica 1
Lecturas	Clases teóricas
Prácticas	Práctica 2
Prácticas	Práctica 3
Tutorías académicas	Tutorías

V.-Tiempo de Trabajo del estudiante	
Clases teóricas	4
Clases de resolución de ejercicios, problemas, casos, etc.	12
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	12
Realización de pruebas	2
Tutorías académicas	9
Actividades relacionadas: jornadas, seminarios, etc.	0
Preparación de clases teóricas	15
Preparación de prácticas/ejercicios/casos	21
Preparación de pruebas	15
Total de horas de trabajo del alumnado	90

VI.-Metodología y plan de trabajo		
Tipo	**Periodo**	**Contenido**
Clases Teóricas	Semana 1 a Semana 15	Impartición de clases magistrales de los temas 1, 2, 3, y 4
Prácticas	Semana 1 a Semana 15	Tras cada uno de los temas se realizará un número de clases prácticas que variará en función del tema.

VII.-Método de evaluación

Evaluación ordinaria continua:
La distribución y características de las pruebas de evaluación son las que se describen a continuación. Solo en casos excepcionales y especialmente motivados, el profesor podrá incorporar adaptaciones en la Guía. Dichos cambios requerirán, previa consulta al Responsable de la Asignatura, la autorización previa y expresa del Coordinador de Grado, quien notificará al Vicerrectorado con competencias en materia de Ordenación Académica la modificación realizada. En todo caso, las modificaciones que se propongan deberán atender a lo establecido en la memoria verificada. Para que tales cambios sean efectivos, deberán ser debidamente comunicados a comienzo de curso a los estudiantes a través del Aula Virtual.
La suma de las actividades no revaluables no podrá superar el 50% de la nota de la asignatura y, en general, no podrán tener nota mínima (salvo en el caso de las prácticas de laboratorio o prácticas clínicas, cuando esté debidamente justificado), evitando incorporar pruebas que superen el 60% de la ponderación de la asignatura.
Evaluación extraordinaria: Los estudiantes que no consigan superar la evaluación ordinaria, o no se hayan presentado, serán objeto de la realización de una evaluación extraordinaria para verificar la adquisición de las competencias establecidas en la guía, únicamente de las actividades de evaluación revaluables.

Descripción de las pruebas de evaluación y su ponderación

Sistema de Evaluación	Revaluable en Extraordinaria	Ponderación	Actividad de evaluación	Nota mínima	Contenidos	Fecha
SE 1 - Prueba escrita de respuesta abierta o tipo test	SI	55%	Prueba escrita	5	Todo el temario	Fecha oficial de convocatoria ordinaria
SE 2 - Resolución de problemas y casos prácticos	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	30%	Práctica 1 (50%)	3	Temas 1, 2, 3	Semana 12
			Práctica 2 (50%)	3	Temas 4 y 5	Semana 14
SE 5 - Participación	NO	15%	Participación en clase	NO	Temario impartido en clase	Durante el curso

Cálculo de la nota final

•La **nota final** se calcula como la **media ponderada** de las notas de las pruebas evaluables según los porcentajes indicados, siempre y cuando se hayan superado con la nota mínima indicada para cada una de ellas.

•Si no se ha presentado a alguna prueba evaluable, la nota final será **"No presentado".**

Convocatoria extraordinaria

En convocatoria extraordinaria los estudiantes solamente se presentarán a la revaluación de las pruebas no superadas, de manera que para el cálculo de la nota final en esta convocatoria se utilizará la calificación de las pruebas aprobadas en convocatoria ordinaria y las notas obtenidas en las pruebas revaluadas. El cálculo de la nota final se realiza tal y como se indica en el apartado anterior.

La revaluación de las pruebas se realizará en la fecha oficial indicada para la convocatoria extraordinaria.

Conducta académica

En el caso de **fraude académico** en alguna actividad de evaluación, se otorgará una calificación de cero puntos en dicha actividad lo que, para aquellas actividades con nota mínima superior a cero implica el suspenso en la convocatoria correspondiente.

Se recuerda además que, atendiendo al artículo 8.g). de la **Normativa de Convivencia de la Universidad Rey Juan Carlos** (https://www.urjc.es/images/Universidad/Presentacion/normativa/normativa%20convivencia%20universitaria.pdf) el **fraude académico** en alguna actividad de evaluación se considera **falta muy grave**. Las sanciones correspondientes a las faltas muy graves, según el artículo 11 de la referida normativa, son la expulsión temporal de la Universidad, y la pérdida en su caso de los derechos de matrícula.

VII.B.-Evaluación de estudiantes con dispensa académica de asistencia a clase

Para que un alumno pueda optar a esta evaluación, tendrá que obtener la 'Dispensa Académica de asistencia a clase' para la asignatura, que habrá solicitado al Decano/a o Director/a del Centro que imparte su titulación. La Dispensa Académica se podrá conceder siempre y cuando las peculiaridades propias de la asignatura lo permitan. Una vez que se haya notificado la concesión de la Dispensa Académica, el docente deberá informar al estudiante a través del Aula Virtual acerca del plan de evaluación establecido en cada caso.

Asignatura con posibilidad de dispensa: Si

VII.C.-Revisión de las pruebas de evaluación

Conforme a la normativa de reclamación de exámenes de la Universidad Rey Juan Carlos.

VII.D.-Estudiantes con discapacidad o necesidades educativas especiales

Las adaptaciones curriculares para estudiantes con discapacidad o con necesidades educativas especiales, a fin de garantizar la igualdad de oportunidades, no discriminación, la accesibilidad universal y la mayor garantía de éxito académico serán pautadas por la Unidad de Atención a Personas con Discapacidad en virtud de la Normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.
Será requisito para ello la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que los estudiantes con discapacidad o necesidades educativas especiales deberán contactar con ella, a fin de analizar conjuntamente las distintas alternativas.

VII.E.-Conducta Académica, integridad y honestidad académica

La Universidad Rey Juan Carlos está plenamente comprometida con los más altos estándares de integridad y honestidad académica, por lo que estudiar en la URJC supone asumir y suscribir los valores de integridad y la honestidad académica recogidos en el Código Ético de la Universidad (https://www.urjc.es/codigoetico). Para acompañar este proceso, la Universidad dispone de la Normativa sobre conducta académica de la Universidad Rey Juan Carlos (https://urjc.es/images/Universidad/Presentacion/normativa/Normativa_conducta_academica_URJC.pdf) y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

VIII.-Recursos y materiales didácticos
Bibliografía básica
Georgia Weidman. *Penetration Testing: A Hands-On Introduction to Hacking*. Ed. no starch press
David Kennedy, Jim O'Gorman, Devon Kearns and Mati Aharoni. *Metasploit: The Penetration Tester's Guide*. Ed. no starch press.
Sagar Rahalkar. *Metasploit 5.0 for Beginners*. Packt Publishing.
Furqan Khan. *Hands-On Penetration Testing with Python.* Packt Publishing.
Forshaw, J. (2024). *Windows security internals / James Forshaw.*
Isakov, D. (2023). *Pentesting Active Directory and Windows-Based Infrastructure: A Comprehensive Practical Guide to Penetration Testing Microsoft Infrastructure / Denis Isakov.* (First).
Bibliografía complementaria

IX.-Profesorado	
Nombre y apellidos	SERGIO PEREZ PELO
Correo electrónico	sergio.perez.pelo@urjc.es
Departamento	Informática y Estadística
Categoría	Profesor/a Ayudante Doctor/a
Titulación académica	Doctor
Responsable de asignatura	Si
Horario de Tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/-a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	1
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	1