

GUÍA DOCENTE PENTESTING

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2026-27

Fecha de publicación: 07-07-2026



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.

II.B-Presentación en inglés

This course aims to be an introductory course to penetration testing. Penetration testing, or pentesting, consists of simulating real-world attacks to assess the risk associated with potential security breaches. The objective is to discover and exploit vulnerabilities to evaluate which assets a potential malicious attacker could gain access to. All phases of a pentest will be studied, from the reconnaissance phase to the privilege escalation and access maintenance phases. This course is taught in the first semester of the fourth year of the degree. To take this course, knowledge from previous subjects will be required, such as hacking techniques, secure web development, secure development methodologies, programming, networking, systems administration, etc

III.-Resultados de Aprendizaje



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.

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.

- Leyenda para las titulaciones no adaptadas al RD 822/21: **CB** - competencias básicas, **CG** - competencias generales, **CE** - competencias específicas, **CT** - competencias transversales.
- Leyenda para las titulaciones adaptadas al RD 822/21: **CON** - conocimientos, **COM** - competencias, **HAB** - habilidades.



IV.-Contenido

IV.A.-Temario de la asignatura

Tema	Descripción
Tema 1: Introducción al Pentesting	Fundamentos básicos de la ciberseguridad. Que es el pentesting o test de penetración. Beneficios, objetivos, utilidad y necesidades de los test de penetración. Comunicación con el cliente. Tipos y alcance de Pentesting: Caja blanca, caja negra, caja gris. Confidencialidad (NDA y contratos). Etapas de un test de penetración.
Tema 2: Herramientas para Pentesters	Clasificación de Herramientas de Pentesting. Comandos. Herramientas y frameworks de pentesting.
Tema 3: Elaboración de Informes	Estructura y Contenido de un Informe de Pentesting. Priorización y Clasificación de Vulnerabilidades. Presentación de Resultados y Comunicación con el Cliente. Tendencias y Evolución del Pentesting.
Tema 4: Desarrollo de Exploits	Fundamentos. Desbordamiento. Desarrollo de Exploit.
Tema 5: Pentesting en entornos web	Introducción al Pentesting en web. Vulnerabilidades Comunes en Aplicaciones web. Herramientas para Pentesting web.
Tema 6: Pentesting en Entornos Móviles	Introducción al Pentesting en entornos móviles. Vulnerabilidades Comunes en entornos Móviles. Herramientas para Pentesting en entornos móviles.
Tema 7: Pentesting en IoT	Introducción al Pentesting en IoT. Vulnerabilidades Comunes en IoT. Herramientas para Pentesting en IoT.
Tema 8: Presente y futuro del Pentesting	Evolución del Pentesting. IA en el Pentesting.

IV.B.-Actividades formativas

Tipo	Descripción
Prácticas	Práctica 1
Tutorías académicas	Práctica 2
Lecturas	Clases teóricas
Tutorías académicas	Tutorías
Realización de pruebas	Examen Teoría Parcial 1: Temas 1-4



Realización de pruebas

Examen Teoría Parcial 2: Temas 5-8

V.-Tiempo de trabajo del alumnado (30h grado y 25h máster)

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, 4, 5, 6, 7 y 8
Prácticas	Semana 1 a Semana 15	Se realizarán dos prácticas durante el curso con evaluación individual mediante examen de prácticas.
Pruebas	Semana 1 a Semana 15	Se realizarán dos exámenes de teoría uno de los temas del 1 al 4 y otro de los temas 5 al 8



VII.-Método de evaluación

El modelo de evaluación general es la evaluación continua, tal como establece el Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

Deberán utilizarse todos los sistemas de evaluación establecidos para la asignatura en la memoria de la titulación, excepto aquellos que tuviesen una ponderación mínima del 0%, que podrán utilizarse en los cursos académicos en los que el profesorado lo considere oportuno. Cada uno de los sistemas de evaluación podrá ser aplicado mediante una o más actividades de evaluación, coherentes con ese sistema. Ninguna de las actividades de evaluación podrá superar individualmente el 60% de la calificación global de la asignatura.

La suma de las actividades de evaluación no revaluables no podrá superar el 40% de la calificación global de la asignatura y, en general, no deberían tener nota mínima (salvo en el caso de actividades de carácter práctico en las que, estrictamente, no pudieran reproducirse en la convocatoria extraordinaria las condiciones de evaluación de la convocatoria ordinaria).

El alumnado que no consiga superar la asignatura en la convocatoria ordinaria, o no se hayan presentado, podrán presentarse a la convocatoria extraordinaria únicamente a las actividades de evaluación revaluables no superadas.

El uso de herramientas basadas en inteligencia artificial está prohibido en cualquier ejercicio y prueba de evaluación de la asignatura salvo que el profesor lo indique de forma explícita en el enunciado o en el material de esta. En caso de que esté permitido, se darán indicaciones precisas de qué usos están permitidos y cuáles no.

La distribución y características de las actividades de evaluación son las que se describen a continuación.

VII.A.- Descripción de las actividades de evaluación y su ponderación

Sistema de evaluación	Actividad de evaluación	Ponderación	Revaluable en extraordinaria	Nota mínima	Contenidos	Fecha
SE1	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria .	Prueba 1 (30%)	Prueba individual y escrita de respuesta abierta o tipo test o selección.	4	Temas 1 al 4	Semana 7 a semana 11
		Prueba 2 (30%)	Prueba individual y escrita de respuesta abierta o tipo test o selección.	4	Temas 5 al 8	Fecha del examen de convocatoria ordinaria
SE 2	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria	Práctica 1 (20%)	Prueba individual y escrita de respuesta abierta o tipo test o selección.	4	Temas 1 al 3	Semana 5 a semana 10
		Práctica 2 (20%)	Prueba individual y escrita de respuesta abierta o tipo test o selección.	4	Temas 4 al 6	Fecha del examen de convocatoria ordinaria

Cálculo de la nota final o global

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. La **nota final** para aprobar deberá ser de 5 puntos sobre 10.

Si alguna de las pruebas o prácticas evaluables no se ha superado con la nota mínima necesaria para hacer media, la nota final de la asignatura será:

- Si la media ponderada ≤ 4 , la nota final será la media ponderada.
- Si la media ponderada > 4 , la nota final será un 4.
- Si no se ha presentado a alguna prueba, se le pondrá un 0 en esa prueba.

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

Convocatoria extraordinaria

En convocatoria extraordinaria los estudiantes solamente se presentarán a la reevaluación de las pruebas y prácticas no superadas, de manera que, para el cálculo de la nota final en esta convocatoria se utilizará la calificación de las pruebas y prácticas aprobadas en convocatoria ordinaria.

En caso de presentarse a una prueba que ya hubiera superado, se mantendrá la nota obtenida en la convocatoria extraordinaria, independientemente de si es superior o inferior a la nota de la convocatoria ordinaria.



Otras observaciones o aclaraciones

Los estudiantes podrán no reevaluarse de las pruebas y prácticas con una calificación ≥ 4 puntos y < 5 puntos, conservando la calificación obtenida en la convocatoria ordinaria.

El cálculo de la nota final en la convocatoria extraordinaria se realizará del mismo modo que en la convocatoria ordinaria.

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

Para la reevaluación de la participación en clase y de las prácticas se planificarán sendos plazos de entrega a determinar dentro de las fechas de exámenes de convocatoria extraordinaria.

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 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 del alumnado con dispensa académica de asistencia a clase

La concesión de Dispensa Académica de Asistencia a Clase (DAAC) no implica que se quede automáticamente eximido de participar en las actividades de evaluación continua ni en las actividades formativas presenciales de asistencia obligatoria establecidas en la guía docente. Una vez concedida la dispensa, el alumnado deberá contactar con el docente, que podría proponerle las adaptaciones que considere convenientes, siempre que garanticen la adquisición y adecuada evaluación de los resultados de aprendizaje previstos. El alumnado deberá mantener a lo largo de curso una comunicación fluida con el docente para que este le proporcione información sobre las fechas en que se realizarán esas actividades formativas y de evaluación, en caso de que su programación no estuviese ya fijada y a disposición del alumnado en el momento de la concesión de la dispensa.

Asignatura con posibilidad de dispensa: Sí

VII.C.- Revisión y reclamación de las actividades de evaluación

Se realizará conforme al Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

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

Con el fin de garantizar la igualdad de oportunidades, la no discriminación, la accesibilidad universal y la mayor garantía de éxito académico, las adaptaciones curriculares para alumnado con discapacidad o con necesidades educativas especiales serán pautadas por la Unidad de Atención a Personas con Discapacidad, de acuerdo con la normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.

Para que esas adaptaciones puedan realizarse, será requisito la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que el alumnado con discapacidad o necesidades educativas especiales deberán contactar con este servicio para analizar conjuntamente las distintas opciones.

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.

Para acompañar este proceso, la Universidad dispone de la Normativa de Convivencia de la Universidad Rey Juan Carlos y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

Las herramientas basadas en inteligencia artificial pueden mejorar la experiencia de aprendizaje, pero debe utilizarse de forma ética, legal, honesta y transparente. Por este motivo, deben seguirse las recomendaciones de uso adecuado indicadas por los docentes de la asignatura.



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.

Bibliografía complementaria

IX.-Profesorado

Nombre y apellidos	JOSÉ DAVID VILLANUEVA GARCÍA
Correo electrónico	josedavid.villanueva@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Asociado/a
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	0
Nombre y apellidos	JUAN MARTÍN MANSILLA
Correo electrónico	juan.martin@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Asociado/a
Responsable de asignatura	Si
Horario de tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico

Nº de Quinquenios	1
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	2