

GUÍA DOCENTE TECNICAS DE HACKING

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2026-27

Fecha de publicación: 19-06-2026



I.-Identificación de la Asignatura	
Tipo	OBLIGATORIA
Período de impartición	2 curso, 1Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

II.-Presentación
La seguridad ofensiva ha cobrado una gran importancia en los últimos años, ya que permite adoptar estrategias de prevención, pero también de detección y de respuesta, comprendiendo las tácticas, técnicas y procedimientos que los adversarios utilizan. En esta asignatura, que es la primera del plan de estudios con este enfoque, se sientan las bases en la materia. Para ello se comienza con un módulo que tiene que ver con la preparación de los ataques, estudiando las técnicas que los adversarios utilizan para recopilar información sobre sus potenciales objetivos, muchas de ellas relacionadas con aspectos tecnológicos pero otras también asociadas al factor humano y que se basan en la ingeniería social. El resto de módulos de la asignatura presentan a los estudiantes técnicas básicas de explotación de vulnerabilidades en Windows y Linux, de ingeniería inversa y desbordamiento de memoria, de inyección de códigos y comandos, de recreación de entornos confiables y suplantación, de interceptación de comunicaciones y Man in the Middle o de denegación de servicio, por mencionar los ejemplos más significativos. Un objetivo muy importante de la asignatura es que los estudiantes adquieran las competencias necesarias para aprender nuevas técnicas de manera autónoma en el futuro, ya que se trata de un campo que evoluciona muy deprisa y en su futura carrera profesional estarán obligados a mantenerse al día con sus propias herramientas y capacidades. Se recomienda haber cursado previamente Introducción a la Ciberseguridad.
II.B-Presentación en inglés

The specific syllabus of the course is as follows: 1. Introduction Offensive security: basic concepts. Anatomy of an attack and kill chain. TTPs, standards and classifications. Ethical hacking. 2. Footprinting and OSINT (non-invasive techniques). Hacking with search engines. Metadata. Other open sources of intelligence. 3. Fingerprinting (invasive techniques). Recognition and enumeration. Traffic analysis. Port and vulnerability scanning. Fuzzing. Anonymity. 4. Social engineering. Techniques that attack the human factor: non-invasive and invasive. Phishing and campaign design. Hacking on the client side (malicious attachments and links, PDFs, USBs, etc.). 5. Basic Windows operating techniques Particularities of Microsoft operating systems and basic hacking (registry, WMI, APIs, PowerShell, etc.). Exploitation of "wormable" vulnerabilities. 6. Basic techniques of exploitation on Linux Particularities of Linux operating systems and basic hacking (kernel vulnerabilities, password attacks). 7. Reverse engineering and overflows. Reverse engineering and code analysis on Windows and Linux. Stack operation. Buffer overflow. Other overflows. 8. Injections and forgeries. Command injection. SQL injection. Other injections. XSS and XSRF. 9. Poisoning, MitM, spoofing and hijacking ARP poisoning and Man in the Middle. Spoofing at different levels. Session hijacking (UDP and TCP hijacking). Denials of service Volumetric denials of service. Attacks on the infrastructure layer: flooding and relays. Attacks on the application layer.

III.-Resultados de Aprendizaje

CG1. Capacidad para resolver problemas con iniciativa, buena toma de decisiones, autonomía y creatividad.

CG3. Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar documentos que tengan por objeto definir, planificar, especificar, resumir proyectos y planes en el ámbito de la ciberseguridad.

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.

CG11. Conocimiento para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos.

CG12. Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad en el ámbito de la ciberseguridad.

CG13. Capacidad para concebir, desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería como instrumento para el aseguramiento de su calidad.

CG15. Capacidad para aplicar conocimientos a su trabajo o vocación de una forma profesional. Capacidad para elaborar y defender argumentos y resolver problemas dentro de su área de estudio.

CG16. Capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CG17. Capacidad para transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CG18. Capacidad para aplicar las habilidades de aprendizaje adquiridas necesarias para emprender estudios posteriores con un alto grado de autonomía.

CE19. Comprender los algoritmos criptográficos de clave pública y de clave privada más importantes y conocer sus aplicaciones en ciberseguridad.

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.

CE26. Conocer los distintos tipos de malware en función de su vector de infección, mecanismos de propagación, replicación y protección, de sus objetivos, etc.

- 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

Bloque	Unidad didáctica	Contenidos
I- Técnicas de recogida de información	1. Introducción	Seguridad ofensiva: conceptos básicos. Anatomía de un ataque y kill chain. TTPs, estándares y clasificaciones. Hacking ético.
	2. Footprinting y OSINT (técnicas no invasivas)	Hacking con buscadores. Metadatos. Otras fuentes abiertas de inteligencia.
	3. Fingerprinting (técnicas invasivas)	Reconocimiento y enumeración. Análisis de tráfico. Escaneo de puertos y de vulnerabilidades. Fuzzing. Anonimato.
	4. Ingeniería social	Técnicas que atacan el factor humano: no invasivas e invasivas. Phishing y diseño de campañas. Hacking en el lado del cliente (adjuntos y links maliciosos, PDFs, USBs, etc.).
II- Hacking de sistemas	5. Técnicas básicas de explotación en Windows	Particularidades de los sistemas operativos de Microsoft y hacking básico (registro, WMI, APIs, PowerShell, etc.). Explotación de vulnerabilidades "wormable".
	6. Técnicas básicas de explotación en Linux	Particularidades de los sistemas operativos de tipo Linux y hacking básico (vulnerabilidades de kernel, ataques a contraseñas).
III- Hacking de aplicaciones tradicionales y web	7. Ingeniería inversa y desbordamientos	Ingeniería inversa y análisis de código en Windows y en Linux. Funcionamiento de la pila. Buffer overflow. Otros desbordamientos.
	8. Inyecciones y forgeries	Inyección de comandos. Inyección SQL. Otras inyecciones. XSS y XSRF.
IV- Hacking de redes y comunicaciones	9. Envenenamientos, MitM, suplantaciones y secuestros	ARP poisoning y Man in the Middle. Spoofing a diferentes niveles. Secuestros de sesión (UDP y TCP hijacking).
	10. Denegaciones de servicio	Denegaciones de servicio volumétricas. Ataques en la capa de infraestructura: inundaciones y reflejos. Ataques en la capa de aplicación.

IV.B.-Actividades formativas

Tipo	Descripción
Prácticas	Resolución de problemas prácticos en ordenador.



Asistencia a clases teóricas	Lecciones magistrales.
Resolución de ejercicios, problemas, casos	Resolución de problemas prácticos en ordenador.
Tutorías académicas	Tutorías.
Realización de Pruebas	Pruebas tipo test y respuesta abierta.
Trabajos individuales	Resolución de problemas prácticos en ordenador.



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

Clases teóricas	22
Clases de resolución de ejercicios, problemas, casos, etc.	10
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	24
Realización de pruebas	4
Tutorías académicas	18
Actividades relacionadas: jornadas, seminarios, etc.	0
Preparación de clases teóricas	30
Preparación de prácticas/ejercicios/casos	42
Preparación de pruebas	30
Total de horas de trabajo del alumnado	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Clases Teóricas	Semana 1 a Semana 16	Clases teóricas donde se explicarán los conceptos de la asignatura.
Resolución de ejercicios, problemas, casos	Semana 3 a Semana 4	Resolución de problemas prácticos en ordenador.
Prácticas	Semana 7 a Semana 8	Resolución de prácticas en ordenador.
Prácticas	Semana 10 a Semana 15	Resolución de prácticas en ordenador.
Prácticas	Semana 1 a Semana 16	Desarrollo de prácticas para profundizar en los contenidos explicados durante las clases de teoría.



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	Reevaluación Extraordinaria	Ponderación	Actividad de Evaluación	Nota mínima	Contenidos	Fecha
SE 1	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	15 %	Pruebas escritas: Resolución de casos, problemas y cuestiones de respuesta abierta	5	Bloque I	Semanas 4 - 8
		45 %	Pruebas escritas: Resolución de casos, problemas y cuestiones de respuesta abierta	5	Bloques II, III y IV	Periodo de exámenes de la ETSII (según calendario académico)
SE 3	Sí. Se seguirá el mismo formato que en convocatoria ordinaria.	20 %	Prácticas con ordenador: Tests/informes y entrega/discusión de resultados (oral e individual)	5	Todo el temario de la asignatura	Durante el cuatrimestre
SE 2	Sí. Se evaluará con un trabajo similar.	20 %	Resolución de problemas y casos prácticos: Informes y entrega/discusión de resultados (oral y colectiva)	5	Técnicas de hacking propuestas por los profesores	Se informará a lo largo del cuatrimestre.

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

Ethical Hacking and Penetration Testing Guide

Rafay Baloch

Auerbach Publications, September 2017

ISBN: 9781351381345

Disponible en la plataforma O'Reilly

Gray Hat Hacking The Ethical Hacker's Handbook (5th Edition)

Stephen Sims, Ryan Linn, Branko Spasojevic, Jonathan Ness, Chris Eagle, Allen Harper, Shon Harris, Daniel Regalado

McGraw-Hill, April 2018

ISBN: 9781260108422

Disponible en la plataforma O'Reilly

Foundations of Cybersecurity, 2nd Edition

A Straightforward Introduction

by Jason Andress

May 2026, 328 pp.

ISBN-13:

9781718504400

Disponible en BRAIN URJC

Linux Basics for Hackers, 2nd Edition

Getting Started with Networking, Scripting, and Security in Kali

Disponible en BRAIN URJC

by OccupyTheWeb

May 2025, 264 pp.

ISBN-13:

9781718503540

Bibliografía complementaria

Learn Ethical Hacking from Scratch

Zaid Sabih

Packt Publishing, July 2018

ISBN: 9781788622059

Disponible en la plataforma O'Reilly

Kali Linux 2018: Assuring Security by Penetration Testing - Fourth Edition

Shakeel Ali, Tedi Heriyanto, Lee Allen, Gerard Johansen, Damian Boodoo, Alex Samm, Shiva V. N Parasram

Packt Publishing, October 2018

ISBN: 9781789341768

Disponible en la plataforma O'Reilly

Hacking For Dummies, 5th Edition

Kevin Beaver

For Dummies, December 2015

ISBN: 9781119154686

Disponible en la plataforma O'Reilly

Practical AI Security

A Hands-on Guide to Attacking, Defending, and Securing Modern AI Systems

by Harriet Farlow

June 2026, 392 pp.

ISBN-13:

9781718504660

Disponible en BRAIN URJC



The Ghidra Book, 2nd Edition
 The Definitive Guide
 by Kara Nance and Chris Eagle
 March 2026, 632 pp.
 ISBN-13:
 9781718504684
 Disponible en BRAIN URJC

IX.-Profesorado	
Nombre y apellidos	RAÚL MARTÍN SANTAMARÍA
Correo electrónico	raul.martin@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Ayudante Doctor/a
Titulación académica	Doctor
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	1
Nº de Sexenios	1
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	1
Nombre y apellidos	SERGIO PÉREZ PELÓ
Correo electrónico	sergio.perez.pelo@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Ayudante Doctor/a
Titulación académica	Doctor
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	1
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	1