

GUÍA DOCENTE TECNICAS DE HACKING

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2024-25

Fecha de publicación: 04-07-2024



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.

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.



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 estudiante (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
Prácticas	Semana 1 a Semana 16	Desarrollo de prácticas para profundizar en los contenidos explicados durante las clases de teoría.
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.



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).

Los estudiantes que no consigan 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.

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

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

Sistema de evaluación	Reevaluable en Extraordinaria	Ponderación	Actividad de Evaluación	Nota mínima	Contenidos	Fecha
SE 1	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	25 %	Pruebas escritas: Resolución de casos, problemas y cuestiones de respuesta abierta	5	Bloque I	Semanas 4 - 8
		30 %	Pruebas escritas: Resolución de casos, problemas y cuestiones de respuesta abierta	5	Bloque 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.	30 %	Prácticas con ordenador: Tests/informes y entrega/discusión de resultados (oral e individual)	5	Todo el temario de la asignatura	Se informará a lo largo del cuatrimestre.
SE 2	Sí. Se evaluará con un trabajo similar.	15 %	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.

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 alguna de las pruebas evaluables no se ha superado con la nota mínima necesaria para hacer media, la nota final de la asignatura será un 3.
- Si no se ha presentado a alguna de las pruebas evaluables en la convocatoria, la nota final será 0.
- 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 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.

Todas las pruebas evaluables en convocatoria extraordinaria mantendrán la misma nota mínima que la indicada para la convocatoria ordinaria.

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

La concesión de Dispensa Académica de Asistencia a Clase (DAAC no implica que el estudiante 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 estudiante 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 estudiante 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 de los estudiantes en el momento de la concesión de la dispensa.

Asignatura con posibilidad de dispensa: Si

VII.C.- Revisión de las pruebas de evaluación

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

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

A fin de garantizar la igualdad de oportunidades, la no discriminación, la accesibilidad universal y la mayor garantía de éxito académico, los y las estudiantes con discapacidad o con necesidades educativas especiales podrán solicitar adaptaciones curriculares para el seguimiento de sus estudios. Esas adaptaciones serán pautadas por la Unidad de Atención a Personas con Discapacidad de la Universidad Rey Juan Carlos, de acuerdo con la normativa que regula el servicio de Atención a Estudiantes con Discapacidad de la Universidad.

Dicha Unidad emitirá un informe de adaptaciones curriculares, por lo que los y las estudiantes con discapacidad o necesidades educativas especiales deberán contactar con la Unidad (discapacidad.programa@urjc.es), 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 de Convivencia de la Universidad Rey Juan Carlos (<https://www.urjc.es/images/Universidad/Presentacion/normativa/normativa%20convivencia%20universitaria.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

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

Bibliografía complementaria

Learn Ethical Hacking from Scratch

Zaid Sabih

Packt Publishing, July 2018

ISBN: 9781788622059

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

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

IX.-Profesorado

Nombre y apellidos	RAÚL MARTÍN SANTAMARÍA
Correo electrónico	raul.martin@urjc.es
Departamento	Informática y Estadística
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
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

