Guía Docente
Curso Académico 2025/26

Datos Generales

Asignatura: HACKING ÉTICO – TEST DE PENETRACIÓN (PENTEST).
Titulación: GRADO EN CIBERSEGURIDAD.
Carácter: OBLIGATORIA.
Créditos ECTS: 6 ECTS.
Curso: 3º
Distribución temporal: 2º SEMESTRE.
Idioma de impartición: CASTELLANO.
Equipo docente: Koldo Gallostra.

Presentación de la asignatura:

Asignatura dedicada a identificar y corregir vulnerabilidades de sistemas informáticos. El alumnado aprende el ciclo de pruebas de penetración —reconocimiento, escaneo, explotación y reporting en entornos de laboratorio controlados. Además, se abordan aspectos éticos y técnicas de ingeniería social.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)

Conocimientos c contenidos (C)	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C3	Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.
	C4	Ejecutar técnicas de desarrollo y penetración analizando las mejoras técnicas, soluciones y buenas prácticas.
	C5	Realizar desarrollos seguros y aplicar contramedidas a nivel de código.
	C13	Analizar la gestión de identidades, cifrado, autenticación, confidencialidad, integridad y disponibilidad de la información.
	C14	Valorar los riesgos que suceda un determinado suceso mediante métodos estadísticos y probabilísticos.
Competencias (CO)	CO1	Usar y programar ordenadores, sistemas operativos, redes, bases de datos y el entorno de la nube para su aplicación en la ciberseguridad.

	CO2	Usar diferentes herramientas de ingeniería y ciberseguridad para la resolución de problemas relacionados con los ciberataques.
	CO3	Llevar a cabo distintos procesos de análisis en las diferentes áreas de la ciberseguridad.
	CO4	Realizar diseños de ingeniería aplicados a la ciberseguridad.
	CO6	Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.
	CO8	Analizar y ejecutar test de penetración en sistemas informáticos.
	CO10	Aplicar técnicas y herramientas de desarrollo seguro para la verificación y validación del software.
	CO14	Comprender las vulnerabilidades de las nuevas tecnologías y aportar soluciones de ciberseguridad.
Habilidades y destrezas (H)	H1	Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.
	H2	Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado.
	H3	Ser hábil en la comunicación, tanto por escrito como oralmente, en inglés.
	H4	Tomar decisiones en el ámbito profesional, aplicando los conocimientos y técnicas adquiridas a lo largo de la actividad académica.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

- Extracción de información (information gathering).
- Despliegue del laboratorio de pruebas.
- Kali Linux.
- Escaneo y enumeración.
- Vulnerabilidades comunes.
- Análisis manual de vulnerabilidades.

- Análisis automatizado.
- Explotación y gestión de vulnerabilidades.
- Introducción al Hacking ético de sistemas y aplicaciones web.

*(*El contenido desarrollado está disponible en la Programación Docente de la asignatura publicada en el Campus Virtual de la Universidad).*

Metodologías Docentes y Actividades Formativas

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudio de casos.
MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	**Horas previstas**	**% presencialidad**
AF1: Clase teórica.	23	100
AF2: Clases en laboratorio.	15	100
AF3: Realización de trabajos (individuales y/o grupales).	12	50
AF4: Tutorías (individuales y/o grupales).	5	50
AF5: Estudio independiente y trabajo autónomo del estudiante.	90	0
AF6: Pruebas de evaluación.	11	100
Total	**156**	

Evaluación: Sistemas y Criterios de Evaluación

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. mín.	Pond. Máx
SE1 Evaluación de la asistencia y participación del estudiante.	0	5
SE6 Evaluación de laboratorios.	10	35
SE3 Pruebas de evaluación y/o exámenes.	50	70

El estudiantado posee dos opciones de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con una convocatoria/año.
- En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiante acogerse a la evaluación única (examen único).
- No se permite el cambio del sistema de evaluación escogido por el estudiante a lo largo del curso.
- El estudiante que desee acogerse a la evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio del curso.
- Si el estudiante no asiste un 80% a las clases presenciales no podrá presentarse a la convocatoria ordinaria y pasará automáticamente a convocatoria extraordinaria.
- Las faltas de asistencia deben justificarse al profesor responsable de la asignatura.
- De manera excepcional, el docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del estudiante, etc. la posibilidad de permitir que el estudiante continué en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.
- El estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

- El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.
    - 0-4,9: Suspenso (SS).
    - 5,0-6,9: Aprobado (AP).
    - 7,0-8,9: Notable (NT).
    - 9,0-10: Sobresaliente (SB)
- La mención de «Matrícula de Honor» podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor»
- Será considerado no presentado (NP) el estudiante matriculado que no realice ninguna actividad evaluativa.
- Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas orto tipográficas en la calificación final.
- El plagio está prohibido tanto en los trabajos como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:
    - Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor para analizar las posibles fuentes de plagio y evaluar si están justificadas.
    - Cualquier trabajo con un índice de similitud superior al 30% no será evaluado.

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
- Stuttard, D., & Pinto, M. (2011). The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws (2nd ed.). Wiley.
- Erickson, J. (2008). Hacking: The Art of Exploitation (2nd ed.). No Starch Press.TBD.

Bibliografía Complementaria

- Kennedy, D., O'Gorman, J., Kearns, P., & Aharoni, A. (2011). *Metasploit: The Penetration Tester's Guide*. No Starch Press.
- Kim, P. (2014). *The Hacker Playbook 2: Practical Guide To Penetration Testing*. CreateSpace Independent Publishing Platform.
- Harper, A., Harris, S., Grispos, G., Rash, J., Baldwin, R., & Nguyen, H. (2010). *Gray Hat Hacking: The Ethical Hacker's Handbook* (2nd ed.). McGraw-Hill Education.
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.

Otros Recursos de Aprendizaje Recomendados

- Pendergast, M. (2016). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* (3rd ed.). No Starch Press.
- Smith, R. (2020). *Blue Team Handbook: Incident Response Edition*. Practical Network Defense.
- Bodmer, S. (2017). *Raspberry Pi for Secret Agents*. No Starch Press.