Guía Docente
Curso Académico 2026/27

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 koldo.gallostra@euneiz.com

Aula(s): Aula informatizada

Presentación de la asignatura:

La asignatura de Hacking Ético tiene como objetivo proporcionar al estudiantado los conocimientos teóricos y las competencias prácticas necesarias para identificar, analizar y explotar vulnerabilidades en sistemas, redes y aplicaciones web desde una perspectiva ética y profesional. Se abordan todas las fases de un test de penetración: desde el reconocimiento y escaneo inicial hasta el hacking de sistemas, aplicaciones web y redes, incluyendo además técnicas de ingeniería social, seguridad en entornos móviles, IoT/OT y cloud. La metodología combina fundamentos teóricos con un enfoque eminentemente práctico, apoyándose en plataformas de entrenamiento como Hack The Box, TryHackMe o PortSwigger, y en herramientas ampliamente utilizadas en la industria. Con esta formación, el alumnado estará preparado para realizar auditorías de seguridad y pruebas de penetración de forma responsable y conforme a los estándares profesionales del sector.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)[1]

Conocimientos c contenidos (C)	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.

[1] La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

	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*

Módulo 1: Introducción al Hacking Ético

• 1.1. Visión general de Ataques Informáticos

• 1.2. Metodologías y Marcos de Hacking

• 1.3. Conceptos de Hacking

Módulo 2. Fase de Reconocimiento y Análisis

• 1.1. Footprinting y Reconocimiento

• 1.2. Escaneo de redes

• 1.3. Enumeración

• 1.4. Análisis de vulnerabilidades

Módulo 3. Hacking de Sistemas

• 2.1. Consiguiendo el Acceso

• 2.2. Escalada de Privilegios

• 2.3. Manteniendo el Acceso

• 2.4. Borrado de Registros

Módulo 4. Hacking Web

• 3.1. Hacking de Servidores

• 3.2. Hacking de Aplicaciones Web

• 3.3. SQL Injection

Módulo 5. Hacking de Redes

• 4.1. Sniffing

• 4.2. Sesion Hijacking

• 4.3. Hacking de de redes Wireless

• 4.4. Evasión de IDS, Firewalls y Honeypots

Módulo 6. Otras técnicas y plataformas

• 5.1. Hacking Plataformas Mobile

- 5.2. Hacking IoT y OT
- 5.3. Ingeniería Social
- 5.4. Cloud Computing
- 5.5. Denial-of-Service

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudios de caso.
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: Clase prácticas.	15	100
AF3: Realización de trabajos (individuales y/o grupales).	12	50
AF3: Tutorías (individuales y/o grupales).	5	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	90	0
AF6: Pruebas de evaluación.	11	100
Total	**150**	--

[2] Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5
SE2 Evaluación de trabajos.	10	35
SE6: Evaluación de laboratorios	50	70

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

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/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 estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de 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 de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continue en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la 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/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas 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/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas…)

Recursos audiovisuales
Material específico de la asignatura
Aula informatizada
Laboratorio Ciberseguridad

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[3]

- 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.

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.