UNIVERSIDAD DE MURCIA

1. Identificación

1.1. De la asignatura

Curso Académico	2024/2025
Titulación	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD / MASTER IN CYBERSECURITY
Nombre de la asignatura	TÉCNICAS DE CIBERATAQUES Y HACKING ÉTICO
Código	7810
Curso	PRIMERO
Carácter	OBLIGATORIA
Número de grupos	1
Créditos ECTS	6.0
Estimación del volumen de trabajo	150.0
Organización temporal	1º Cuatrimestre
Idiomas en que se imparte	Inglés

1.2. Del profesorado: Equipo docente

RUIZ MARTINEZ, ANTONIO

Docente: **GRUPO 1**

Coordinación de los grupos: **GRUPO 1**

Coordinador de la asignatura

Categoría
PROFESORES TITULARES DE UNIVERSIDAD

Área
INGENIERÍA TELEMÁTICA

Departamento
INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Correo electrónico / Página web / Tutoría electrónica

arm@um.es https://webs.um.es/arm/ Tutoría electrónica: **Sí**

Teléfono, horario y lugar de atención al alumnado

Duración:	Día:	Horario:	Lugar:
C2	Jueves	17:00-19:00	868887863, Facultad de Informática B1.1.044

Observaciones:
Despacho 1.32 de la Facultad de Informática

Duración:	Día:	Horario:	Lugar:
C2	Viernes	12:00-13:30	868887863, Facultad de Informática B1.1.044

Observaciones:
Despacho 1.32 de la Facultad de Informática

Duración:	Día:	Horario:	Lugar:
C1	Viernes	16:00-17:30	868887863, Facultad de Informática B1.1.044

Observaciones:
Despacho 1.32 de la Facultad de Informática

Duración:	Día:	Horario:	Lugar:
C1	Martes	12:00-13:30	868887863, Facultad de Informática B1.1.044

Observaciones:
Despacho 1.32 de la Facultad de Informática

GOMEZ MARMOL, FELIX

Docente: **GRUPO 1**

Coordinación de los grupos:

Categoría

PROFESORES TITULARES DE UNIVERSIDAD

Área

CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL

Departamento

INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Correo electrónico / Página web / Tutoría electrónica

felixgm@um.es https://webs.um.es/felixgm/ Tutoría electrónica: **Sí**

Teléfono, horario y lugar de atención al alumnado

Duración:	Día:	Horario:	Lugar:
C1	Lunes	15:00-18:00	868889782, Facultad de Informática B1.1.034

Observaciones:
Despacho 1.23, primera planta Facultad de Informática

Duración:	Día:	Horario:	Lugar:
C2	Martes	15:30-18:30	868889782, Facultad de Informática B1.1.034

Observaciones:
Despacho 1.23, primera planta Facultad de Informática

HERNANDEZ RAMOS, JOSE LUIS

Docente: **GRUPO 1**

Coordinación de los grupos:

Categoría
PROFESOR PERMANENTE LABORAL

Área
INGENIERÍA TELEMÁTICA

Departamento
INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Correo electrónico / Página web / Tutoría electrónica
jluis.hernandez@um.es Tutoría electrónica: **No**

Teléfono, horario y lugar de atención al alumnado

NESPOLI, PANTALEONE

Docente: **GRUPO 1**

Coordinación de los grupos:

Categoría
INVESTIGADOR DOCTOR

Área
CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL

Departamento
INGENIERÍA Y TECNOLOGÍA DE COMPUTADORES

Correo electrónico / Página web / Tutoría electrónica
pantaleone.nespoli@um.es Tutoría electrónica: **No**

Teléfono, horario y lugar de atención al alumnado

PEREZ PALMA, NOELIA MARIA

Docente: **GRUPO 1**

Coordinación de los grupos:

Categoría
INVESTIGADOR DOCTOR

Área
No consta

Departamento
INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Correo electrónico / Página web / Tutoría electrónica
noelia.perez3@um.es Tutoría electrónica: **No**

Teléfono, horario y lugar de atención al alumnado

2. Presentación

El objetivo de este curso es que los estudiantes sean capaces de llevar a cabo diferentes procesos relacionados con el ataque a sistemas informáticos y los procesos de hacking ético asociados. Con este fin, la asignatura abordará las diferentes fases que tienen lugar en un proceso de hacking ético, y a través de prácticas de laboratorio, se llevarán a cabo las distintas fases del proceso para que los estudiantes se familiaricen con ellas.

3. Condiciones de acceso a la asignatura

3.1. Incompatibilidades

No constan

3.2. Requisitos

No constan

3.3. Recomendaciones

No existen recomendaciones para esta asignatura.

4. Competencias

4.1. Competencias básicas

- CB9: Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

4.2. Competencias de la titulación

- CG1: Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.
- CG2: Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.
- CG3: Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
- CG4: Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- CE1: Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.

4.3. Competencias transversales y de materia

No constan

5. Contenidos

5.1. Teoría

Tema 1: Fundamentos de hacking ético

Esta unidad cubre los conceptos esenciales relacionados con el hacking ético, incluyendo cuestiones éticas, modelos de ataque, metodologías y diferentes formas de realizar entrenamientos en hacking ético.

Tema 2: Footprinting y reconocimiento

En esta unidad explicamos cómo se puede realizar el footprinting y el reconocimiento mediante el uso de técnicas de inteligencia de fuentes abiertas (OSINT). También presentamos las principales herramientas.

Tema 3: Escaneo de redes

En esta unidad, abordamos temas relacionados con el escaneo de redes, como el descubrimiento de hosts, el escaneo de puertos, el escaneo de vulnerabilidades y las técnicas de evasión.

Tema 4: Enumeración

En esta unidad explicamos cómo podemos realizar la enumeración en diferentes servicios.

Tema 5: Explotación

En esta unidad abordamos las diferentes formas en que podemos aprovechar para realizar la explotación de un sistema o servicio.

Tema 6: Post-explotación

La unidad cubre las diferentes tareas que podemos realizar una vez que hemos llevado a cabo la explotación, es decir, tareas de post-explotación como la enumeración local, la escalada de privilegios, el pivoting y el encubrimiento de huellas.

Tema 7: Informes

La unidad analiza los diferentes aspectos que deben tenerse en cuenta al generar un informe de pentesting una vez que se han desarrollado las fases de pentesting.

5.2. Prácticas

- ### Práctica 1: Footprinting and reconnaisance

  El objetivo de este laboratorio es trabajar con herramientas OSINT para recopilar información de una organización o de usuarios dentro de una organización.

  Relacionado con:

  - Tema 2: Footprinting y reconocimiento

- ## Práctica 2: Escaneo de redes

  Relacionado con:

  - Tema 3: Escaneo de redes

- ## Práctica 3: Active Directory

  Los objetivos principales de esta sesión son comprender los conceptos de escaneo y enumeración en Active Directory y obtener información sobre las herramientas y cmdlets de PowerShell para la enumeración.

  Relacionado con:

  - Tema 3: Escaneo de redes
  - Tema 4: Enumeración

- ## Práctica 4: Explotación

  El objetivo de este laboratorio es adquirir conocimientos sobre explotación, enfocándose específicamente en los temas de búsqueda de exploits, compromiso del sistema, realización de diferentes tipos de ataques, recopilación de información sensible y el arte de romper contraseñas.

  Relacionado con:

  - Tema 5: Explotación

- ## Práctica 5: Post-explotación

  El objetivo de este laboratorio es desarrollar diferentes tareas que se llevan a cabo una vez que hemos comprometido un sistema.

  Relacionado con:

  - Tema 6: Post-explotación

- ## Práctica 6: Informes

  El objetivo de este laboratorio es desarrollar un informe de pentesting

  Relacionado con:

  - Tema 7: Informes

6. Actividades Formativas

Actividad Formativa	Metodología	Horas	Presencialidad
A10: Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría	Ver 8 Sistemas de evaluación	4.0	0.0

o prácticas.

AF1: Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	Durante las sesiones teóricas síncronas, se trabajarán las principales dudas y preguntas que hayan surgido del trabajo realizado en las horas asíncronas (AF3), aplicando una metodología basada en el Aula Invertida (MD6). Además, durante esta actividad formativa, se realizarán cuestionarios para calificar para la Evaluación Continua de este curso. Si es necesario, también se trabajará en la resolución de problemas y ejercicios (MD3).	9.0	0.0
AF2: Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	Durante las sesiones de laboratorio sincrónicas, se explicarán los laboratorios prácticos del curso y/o los estudiantes trabajarán en sus prácticas para resolver dudas.	9.0	0.0
AF3: Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	Estas horas están dedicadas al trabajo previo del estudiante al aplicar la metodología de Aula Invertida (MD6). En este caso, el estudiante debe trabajar de antemano en las tareas planificadas cada semana (ver videos, leer informes, etc.). El trabajo sobre este material también formará parte de la Evaluación Continua del estudiante.	9.0	0.0
AF4: Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	Se explicarán los laboratorios prácticos del curso (y el contenido práctico y/o las herramientas asociadas a estos laboratorios) y/o los estudiantes trabajarán en sus prácticas.	9.0	0.0
AF6: Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	Horas dedicadas a la resolución de dudas de forma individual o en grupo. También pueden dedicarse a ejercicios (MD3).	4.0	0.0
AF8: Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden	Seminarios o clases magistrales (MD1) para profundizar en varios temas necesarios para el desarrollo de los laboratorios.	4.0	0.0

consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.			
AF9: Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	Trabajo autónomo del estudiantado.	102.0	0.0
	Totales	150,00	

7. Horario de la asignatura

https://www.um.es/en/web/estudios/masteres/ciberseguridad/2024-25#horarios

8. Sistemas de Evaluación

Identificador	Denominación del instrumento de evaluación	Criterios de Valoración	Ponderación
IE1	Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	La evaluación continua consiste en la realización de tareas semanales que pueden ser de diferentes tipos: cuestionarios, ejercicios, informes, etc.	20.0
IE2	Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.		0.0
IE3	Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	Individual or group interview assessment on practical laboratories where students will be asked about the laboratories developed and the reports generated. In order to pass the course, this interview is compulsory for each student and the grade of the personal or group interview (PI) must be greater or equal to 5.	50.0
IE4	Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.		30.0

9. Fechas de exámenes

https://www.um.es/en/web/estudios/masteres/ciberseguridad/2024-25#examenes

10. Resultados del Aprendizaje

- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido
- Analizar métodos y técnicas de ciberataques y ciberdefensa
- Diseñar, desplegar y mantener sistemas de ciberseguridad
- Identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad
- Enumerar e identificar los distintos tipos de vulnerabilidades, amenazas y riesgos dentro de la organización, así como posibles soluciones a aplicar
- Realizar procesos de análisis de vulnerabilidades y de riesgos
- Clasificar las vulnerabilidades, amenazas y riesgos dentro de la organización para determinar su importancia teniendo en cuenta el contexto

11. Bibliografía

Grupo: GRUPO 1

Bibliografía básica

- CEH v12 - Certified Ethical Hacker - Study Guide. Sybex

Bibliografía complementaria

- M. G. Solomon, S-P. Oriyano, "Ethical Hacking: Techniques, Tools, and Countermeasures, Fourth Edition". Jones & Bartlett Learning.

12. Observaciones

(**) Evaluación

Esta asignatura se puede aprobar a través de los mecanismos de Evaluación Continua (CA), Informes de Laboratorio (LR) y Entrevista Personal o Grupal (PI). La fórmula para la evaluación es la siguiente: 0,2CA + 0,5LR + 0,3*PI, siempre y cuando el estudiante apruebe tanto LR como PI. De lo contrario, se calificará con un 4 si ha participado en todos los mecanismos de evaluación, o como "No Presentado" si alguno de los mecanismos de evaluación no se ha llevado a cabo.

Esta asignatura no está directamente vinculada con los Objetivos de Desarrollo Sostenible (ODS).

NECESIDADES EDUCATIVAS ESPECIALES

Aquellos estudiantes con discapacidad o necesidades educativas especiales podrán dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV - https://www.um.es/adyv) para recibir orientación sobre un mejor aprovechamiento de su proceso formativo y, en su caso, la adopción de medidas de equiparación y de mejora para la inclusión, en virtud de la Resolución Rectoral R-358/2016. El tratamiento de la información sobre este alumnado, en cumplimiento con la LOPD, es de estricta confidencialidad.

REGLAMENTO DE EVALUACIÓN DE ESTUDIANTES

El artículo 8.6 del Reglamento de Evaluación de Estudiantes (REVA) prevé que "salvo en el caso de actividades definidas como obligatorias en la guía docente, si el o la estudiante no puede seguir el proceso de evaluación continua por circunstancias sobrevenidas debidamente justificadas, tendrá derecho a realizar una prueba global".

Se recuerda asimismo que el artículo 22.1 del Reglamento de Evaluación de Estudiantes (REVA) estipula que "el o la estudiante que se valga de conductas fraudulentas, incluida la indebida atribución de identidad o autoría, o esté en posesión de medios o instrumentos que faciliten dichas conductas, obtendrá la calificación de cero en el procedimiento de evaluación y, en su caso, podrá ser objeto de sanción, previa apertura de expediente disciplinario".