1. General information

Course: SECURITY IN COMPUTING SYSTEMS	**Code:** 42357
Type: ELECTIVE	**ECTS credits:** 6
Degree: 406 - UNDERGRADUATE DEGREE IN COMPUTER SCIENCE AND ENGINEERING (AB)	**Academic year:** 2023-24
Center: 604 - SCHOOL OF COMPUTER SCIENCE AND ENGINEERING (AB)	**Group(s):** 13
Year: 4	**Duration:** First semester
Main language: Spanish	**Second language:** English
Use of additional languages:	**English Friendly:** Y
Web site:	**Bilingual:** N

Lecturer: JOSE LUIS MARTINEZ MARTINEZ - Group(s): **13**

Building/Office	Department	Phone number	Email	Office hours
ESII-1.C.11	SISTEMAS INFORMÁTICOS	2294	joseluis.martinez@uclm.es	

2. Pre-Requisites

Mandatory subject for the Technology Specific Information Technology Subject, it is advisable to have completed the Basic Training modules and the Common module to the Computing Branch (Modules I and II). It is therefore recommended to have clear the basic c

3. Justification in the curriculum, relation to other subjects and to the profession

This subject is integrated in the subject of Technologies and Information Systems of the curriculum.

Computer security is a common competence in all the Computer Engineering plans, included in the White Paper and in all IEEE / ACM curricular recommendations.

Safety is a specific competence, but it affects all subjects in the curriculum. The weak link principle states that a computer system is as safe as its most vulnerable point. This necessarily translates into a multidisciplinary subject, where aspects of very low level and as

4. Degree competences achieved in this course

Course competences

Code	Description
INS02	Organising and planning skills.
INS05	Argumentative skills to logically justify and explain decisions and opinions.
PER02	Ability to work in multidisciplinary teams.
SIS01	Critical thinking.
SIS03	Autonomous learning.
SIS04	Adaptation to new scenarios.
SIS05	Creativity.
TI07	Ability to understand, apply, and manage the reliability and safety of digital systems.

5. Objectives or Learning Outcomes

Course learning outcomes

Description
Identification of vulnerabilities in the computer system, analyze and classify attacks.
Configuration of secure networks using firewalls and virtual private networks.
Use of encryption and cryptography techniques to protect information.
Management of security in computing systems.
Design of security and contingency plans in Data Processing Centers (DPCs).
Knowledge about the latest techniques in transaction security, as well as current legislation regarding data protection.

6. Units / Contents

Unit 1: Introduction
    Unit 1.1 Presentation
    Unit 1.2 Introduction to Information Security
    Unit 1.3
Unit 2: Ethical Hacking
    Unit 2.1 Footprinting & Open Source Inteligence
    Unit 2.2 Fingerprinting & Enumeration
    Unit 2.3 NavajaNegra Conference
Unit 3: Web Auditory
    Unit 3.1 OWASP & Proxy Web
    Unit 3.2 XSS
    Unit 3.3 CSRF+LFI+RFI+CLI
Unit 4:
    Unit 4.1
    Unit 4.2
    Unit 4.3
    Unit 4.4
Unit 5:
    Unit 5.1
    Unit 5.2
    Unit 5.3
    Unit 5.4
    Unit 5.5

7. Activities, Units/Modules and Methodology

Training Activity	Methodology	Related Competences (only degrees before RD 822/2021)	ECTS	Hours	As	Com	Description
Class Attendance (theory) [ON-SITE]	Combination of methods	TI07	0.96	24	N	-	
Class Attendance (practical) [ON-SITE]	Practical or hands-on activities	TI07	1.2	30	N	-	
Project or Topic Presentations [ON-SITE]	Group Work	INS02 INS05 PER02 SIS01 SIS03 SIS04 SIS05	0.12	3	Y	N	
Final test [ON-SITE]	Assessment tests	INS05 SIS01	0.2	5	Y	Y	
Writing of reports or projects [OFF-SITE]	Group Work	INS02 INS05 PER02 SIS01 SIS03 SIS04 SIS05	0.8	20	Y	N	
Study and Exam Preparation [OFF-SITE]	Self-study	INS02 INS05 PER02 SIS01 SIS03 SIS04 SIS05 TI07	2.56	64	N	-	
On-line Activities [OFF-SITE]	Assessment tests	INS02 SIS04	0.16	4	Y	N	
		Total:	6	150			

Total credits of in-class work: 2.48	Total class time hours: 62
Total credits of out of class work: 3.52	Total hours of out of class work: 88

As: Assessable training activity
Com: Training activity of compulsory overcoming (It will be essential to overcome both continuous and non-continuous assessment).

8. Evaluation criteria and Grading System

Evaluation System	Continuous assessment	Non-continuous evaluation*	Description
Final test	25.00%	50.00%	
Final test	25.00%	50.00%	
Progress Tests	50.00%	0.00%	
Total:	**100.00%**	**100.00%**	

According to art. 4 of the UCLM Student Evaluation Regulations, it must be provided to students who cannot regularly attend face-to-face training activities the passing of the subject, having the right (art. 12.2) to be globally graded, in 2 annual calls per subject , an ordinary and an extraordinary one (evaluating 100% of the competences).

Evaluation criteria for the final exam:
    Continuous assessment:
        [MODALITY WITH CONTINUOUS EVALUATION]

-Theory:
- Theoretical Final Examination: 25% (Minimum score: 4 points, Compensable with the tests of the continuous assessment)
-Practices:
- Practical Laboratory Final Exam: 25% (Minimum score: 4 points) Compensable with the tests of the continuous evaluation
-Continuous assessment:
Test Evaluables: 40% A test of 10 V / F questions will be carried out at the end of each sub-topic.
- Job:
- Practical work defended in class: 10%

[MODALITY WITHOUT CONTINUOUS EVALUATION]
-Theory:
- Final Exam: 50% (Minimum score: 4 points, Compensable with the practical part)
-Practices:
- Final Exam of Practices: 50% (Minimum score: 4 points, Compensable with the theory part)

In both modalities, each part is saved for the extraordinary call if it exceeds 5

The student who does not pass all the minimum required tests (minimum score of 4 both in the theory and practical exam) in the subject will appear as a failure and will have a final grade corresponding to the average grade between the theory and practice exam. In case the average of approved, will have a note of suspense, 4.

Non-continuous evaluation:
Evaluation criteria not defined

Specifications for the resit/retake exam:
In the extraordinary call only the final theory exam and the practical case in the laboratory can be recovered, the test and work notes are kept from the ordinary one. If the student wishes, it can be presented according to the format WITH OR WITHOUT CONTINUOUS EVALUATION MODALITY, that is, with or without taking into account the results of the continuous evaluation.

Specifications for the second resit / retake exam:
Same as the extraordinary

9. Assignments, course calendar and important dates	
Not related to the syllabus/contents	
Hours	**hours**
Project or Topic Presentations [PRESENCIAL][Group Work]	3
Final test [PRESENCIAL][Assessment tests]	5
Writing of reports or projects [AUTÓNOMA][Group Work]	4
Study and Exam Preparation [AUTÓNOMA][Self-study]	5
Unit 1 (de 5): Introduction	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	4
Study and Exam Preparation [AUTÓNOMA][Self-study]	2
Unit 2 (de 5): Ethical Hacking	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	4
Class Attendance (practical) [PRESENCIAL][Practical or hands-on activities]	4
Writing of reports or projects [AUTÓNOMA][Group Work]	16
Study and Exam Preparation [AUTÓNOMA][Self-study]	11
Unit 3 (de 5): Web Auditory	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	4
Class Attendance (practical) [PRESENCIAL][Practical or hands-on activities]	4
Study and Exam Preparation [AUTÓNOMA][Self-study]	13
On-line Activities [AUTÓNOMA][Assessment tests]	1
Unit 4 (de 5):	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	6
Class Attendance (practical) [PRESENCIAL][Practical or hands-on activities]	9
Study and Exam Preparation [AUTÓNOMA][Self-study]	11
On-line Activities [AUTÓNOMA][Assessment tests]	1
Unit 5 (de 5):	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	6
Class Attendance (practical) [PRESENCIAL][Practical or hands-on activities]	13
Study and Exam Preparation [AUTÓNOMA][Self-study]	22
On-line Activities [AUTÓNOMA][Assessment tests]	2
Global activity	
Activities	**hours**
Class Attendance (practical) [PRESENCIAL][Practical or hands-on activities]	30
Project or Topic Presentations [PRESENCIAL][Group Work]	3
Final test [PRESENCIAL][Assessment tests]	5
Writing of reports or projects [AUTÓNOMA][Group Work]	20
Study and Exam Preparation [AUTÓNOMA][Self-study]	64
On-line Activities [AUTÓNOMA][Assessment tests]	4
Class Attendance (theory) [PRESENCIAL][Combination of methods]	24
Total horas:	150

10. Bibliography and Sources							
Author(s)	**Title/Link**	**Publishing house**	**Citv**	**ISBN**		**Year**	**Description**
Kurose, J., Ross, K.	Redes de Computadores. Un enfoque descendente basado en Internet	Pearson Education				2003	
William Stallings	Computer security. Principles and Practice	Pearson International Edition				2008	
William Stallings	Fundamentos de seguridad en redes	Pearson Prentice Hall				2003	
varios	Colección Pack Completa http://0xword.com/es/	0xword					Colección de varios ejemplares
Fundamentos de Seguridad en Redes	Fundamentos de Seguridad en Redes	Cisco Press				2008	