UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. General information

Course:	SECURITY IN COMMUNICATIONS	**Code:**	59664
Type:	ELECTIVE	**ECTS credits:**	6
Degree:	385 - DEGREE IN TELECOMMUNICATI TECHNOLOGY ENGINEERING	**Academic year:**	2023-24
Center:	308 - SCHOOL POLYTECHNIC OF CUENCA	**Group(s):**	30
Year:	4	**Duration:**	First semester
Main language:	Spanish	**Second language:**	
Use of additional languages:		**English Friendly:**	Y
Web site:		**Bilingual:**	N

Lecturer: **JOSE ANTONIO BALLESTEROS GARRIDO** - Group(s): **30**

Building/Office	**Department**	**Phone number**	**Email**	**Office hours**
E. Politécnica Cuenca (2.16)	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, AUTOMÁTICA Y COMUNICACIONES	926053863	josea.ballesteros@uclm.es	Office hours will be published at "secretaria virtual"

2. Pre-Requisites

It is advisable to study previously the courses 'Communication Networks I', 'Communication Networks II', 'Processing and Transmission'. Students should know: TCP/IP protocols, local area networks, network interconection devices, routing protocols, VLANs and cryptography.

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

Communication security is one of the working areas for Telecommunication Engineers in public and private companies due to an increasing number of ciberattacks to people, companies, administrations, states, etc.

4. Degree competences achieved in this course

Course competences

Code	Description
E26	The ability to construct, use and manage telecommunication networks, services, processes and applications, which are defined as systems for capturing, transporting, representing, processing, storing, managing and presenting multimedia information, from the viewpoint of transmission systems.
E31	The ability to analyse, encode, process and transmit multimedia information using analogue and digital signal processing techniques.
G02	Correct, oral and written, communication skills.
G06	Knowledge of basic subjects and technologies, enabling students to learn new methods and technologies, as well as providing great versatility to adapt to new situations
G07	The ability to tackle problems with initiative, making decisions, creativity, and to communicate and transmit knowledge, skills and abilities, including the ethical and professional responsibility of the activity of a Technical Telecommunications Engineer
G08	Knowledge to perform measurements, calculations, assessments, appraisals, surveys, studies, reports, task planning and other similar work in their specific telecommunications field
G13	The ability to look for and understand information, wether technical or commercial in different sources, to relate and structure it to integrate ideas and knowledge. Analysis, synthesis and implementation of ideas and knowledge.

5. Objectives or Learning Outcomes

Course learning outcomes

Description

Knowledge and respect of professional ethics and deontology.

Analysis, synthesis and compression of technical documentation and mastery of specific vocabulary.

Synthesis of capacities of several telecommunications engineering areas.

Correct use of oral and written expression to convey ideas, technologies, results, etc.

Application of telecommunication systems in various fields of engineering.

Use of ICT to achieve the specific objectives set in the subject.

6. Units / Contents

Unit 1: Introduction

- **Unit 1.1** Law
- **Unit 1.2** Introduction to cybersecurity and cyberattacks
- **Unit 1.3** Cryptography applications
- **Unit 1.4** Esteganography
- **Unit 1.5** Laboratory 1: Cryptography applications

Unit 2: Pentesting

- **Unit 2.1** Introduction to pentesting

- **Unit 2.2** Information gathering
- **Unit 2.3** Attack
- **Unit 2.4** Recommendations
- **Unit 2.5** Report
- **Unit 2.6** Pentesting devices
- **Unit 2.7** Laboratory 2: Pentesting tools

Unit 3: OSINT and Hacking with Search Engines

- **Unit 3.1** OSINT
- **Unit 3.2** Hacking with Search Engines: Google, Bing, Shodan, Robtex
- **Unit 3.3** Laboratory 3: Researching process with OSINT techniques

Unit 4: Security in Local Area Networks

- **Unit 4.1** Security Measurements
- **Unit 4.2** Sniffers
- **Unit 4.3** Attacks in LAN
- **Unit 4.4** Attacks Protection
- **Unit 4.5** Laboratory 4: Attacks in Local Area Networks

Unit 5: Security in WiFi networks

- **Unit 5.1** WiFi Security
- **Unit 5.2** Attacks in WiFi Networks
- **Unit 5.3** Fake AP
- **Unit 5.4** Laboratory 5: Attacks in WiFi Networks

ADDITIONAL COMMENTS, REMARKS

Software: GNS3, Kali linux.

Hardware: Router, Switch

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]	Lectures	E26 E31 G02 G06 G08	0.75	18.75	N	-	Lectures and demos to explain the learning outcomes
Problem solving and/or case studies [ON-SITE]	Problem solving and exercises	E31 G02 G06 G07 G08	0.7	17.5	Y	N	During the course, some activities will be proposed. The answer to these activities will be presented in pdf format. If plagiarism is detected, the student will have a mark equal to 0 points.
Writing of reports or projects [OFF-SITE]	Problem solving and exercises	E31 G02 G06 G07 G08	1	25	Y	N	During the course, some activities will be proposed. The answer to these activities will be presented in pdf format. If plagiarism is detected, the student will have a mark equal to 0 points.
Laboratory practice or sessions [ON-SITE]	Practical or hands-on activities	E26 E31 G02 G06 G07 G08 G13	0.7	17.5	Y	N	During the laboratory sessions, the process and results obtained will be evaluated
Practicum and practical activities report writing or preparation [OFF-SITE]	Practical or hands-on activities	E26 E31 G02 G06 G07 G08 G13	0.5	12.5	Y	N	Reports will be presented in pdf format including comments to the questions specified in the statement. Apart from that, other program files will also be requiered. If plagiarism is detected, the student will have a mark equal to 0 points.
Study and Exam Preparation [OFF-SITE]	Combination of methods	E26 E31 G02 G06 G07 G08 G13	2.1	52.5	N	-	Autonomous study
Individual tutoring sessions [ON-SITE]	Combination of methods	E26 E31 G02 G06 G07 G08 G13	0.08	2	N	-	Session for doubts and task review
Final test [ON-SITE]	Assessment tests	E26 E31 G02 G06 G07 G08 G13	0.17	4.25	Y	N	Practice exam (CTF) and a test. Exams will be retaken with another realization. If plagiarism is detected the student will have a mark equal to 0 points.
		Total:	**6**	**150**			
		Total credits of in-class work: 2.4					**Total class time hours: 60**
		Total credits of out of class work: 3.6					**Total hours of out of class work: 90**

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

Assessment of problem solving and/or case studies	10.00%	10.00%	Reports during the course
Laboratory sessions	65.00%	65.00%	In-situ work in laboratory and written reports
Final test	25.00%	25.00%	Practice exam (CTF) and a test
Oral presentations assessment	10.00%	0.00%	Optional and Voluntary activity. Students can do an oral presentation of a PoC that will be rewarded with an extra mark up to 1 point
Total:	**110.00%**	**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:

Those described in the 'evaluation system' table

Non-continuous evaluation:

Those described in the 'evaluation system' table

Specifications for the resit/retake exam:

Activities will be retaken individually with another realization.
The final test will be retaken with another test.
The evaluation criteria will be those described in the 'evaluation system' table.

Specifications for the second resit / retake exam:

The final test will be retaken with another test.
If the student passed the laboratory sessions in advance, the evaluation criteria will be 70% laboratory sessions and 30% writing test. In other case, activities will be retaken individually with another realization and the evaluation criteria will be 70% laboratory sessions and 30% writing test

9. Assignments, course calendar and important dates

Not related to the syllabus/contents	
Hours	**hours**
Study and Exam Preparation [AUTÓNOMA][Combination of methods]	52.5
Individual tutoring sessions [PRESENCIAL][Combination of methods]	2
Final test [PRESENCIAL][Assessment tests]	4.25
General comments about the planning: Course calendar will be published at the begining of the course	
Unit 1 (de 5): Introduction	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Lectures]	3
Problem solving and/or case studies [PRESENCIAL][Problem solving and exercises]	3.5
Writing of reports or projects [AUTÓNOMA][Problem solving and exercises]	5
Laboratory practice or sessions [PRESENCIAL][Practical or hands-on activities]	3.5
Practicum and practical activities report writing or preparation [AUTÓNOMA][Practical or hands-on activities]	2.5
Unit 2 (de 5): Pentesting	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Lectures]	4
Problem solving and/or case studies [PRESENCIAL][Problem solving and exercises]	3.5
Writing of reports or projects [AUTÓNOMA][Problem solving and exercises]	5
Laboratory practice or sessions [PRESENCIAL][Practical or hands-on activities]	3.5
Practicum and practical activities report writing or preparation [AUTÓNOMA][Practical or hands-on activities]	2.5
Unit 3 (de 5): OSINT and Hacking with Search Engines	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Lectures]	4
Problem solving and/or case studies [PRESENCIAL][Problem solving and exercises]	3.5
Writing of reports or projects [AUTÓNOMA][Problem solving and exercises]	5
Laboratory practice or sessions [PRESENCIAL][Practical or hands-on activities]	3.5
Practicum and practical activities report writing or preparation [AUTÓNOMA][Practical or hands-on activities]	2.5
Unit 4 (de 5): Security in Local Area Networks	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Lectures]	4
Problem solving and/or case studies [PRESENCIAL][Problem solving and exercises]	3.5
Writing of reports or projects [AUTÓNOMA][Problem solving and exercises]	5
Laboratory practice or sessions [PRESENCIAL][Practical or hands-on activities]	3.5
Practicum and practical activities report writing or preparation [AUTÓNOMA][Practical or hands-on activities]	2.5
Unit 5 (de 5): Security in WiFi networks	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Lectures]	3.75
Problem solving and/or case studies [PRESENCIAL][Problem solving and exercises]	3.5
Writing of reports or projects [AUTÓNOMA][Problem solving and exercises]	5
Laboratory practice or sessions [PRESENCIAL][Practical or hands-on activities]	3.5
Practicum and practical activities report writing or preparation [AUTÓNOMA][Practical or hands-on activities]	2.5
Global activity	
Activities	**hours**
Final test [PRESENCIAL][Assessment tests]	4.25

Class Attendance (theory) [PRESENCIAL][Lectures]	18.75
Problem solving and/or case studies [PRESENCIAL][Problem solving and exercises]	17.5
Writing of reports or projects [AUTÓNOMA][Problem solving and exercises]	25
Laboratory practice or sessions [PRESENCIAL][Practical or hands-on activities]	17.5
Practicum and practical activities report writing or preparation [AUTÓNOMA][Practical or hands-on activities]	12.5
Study and Exam Preparation [AUTÓNOMA][Combination of methods]	52.5
Individual tutoring sessions [PRESENCIAL][Combination of methods]	2
Total horas:	150

10. Bibliography and Sources

Author(s)	Title/Link	Publishing house	Citv	ISBN	Year	Description
Rambla, Juan Luis G.	Ataques en redes de datos IPv4 e IPv6 / Juan Luis García Ram	ZeroXword Computing,		978-84-617-9278-8	2018	
Santo Orcero, David	Kali linux /	RA-MA,		978-84-9964-729-6	2018	
Astudillo B., Karina	Hacking Ético : !cómo convertirse en hacker ético en 21 días	RA-MA,		978-84-9964-767-8	2018	
Ramos Varón, Antonio Ángel	Hacking práctico de redes wifi y radiofrecuencia /	Ra-Ma,		978-84-9964-296-3	2015	
Ramos Varón, Antonio Ángel	Seguridad perimetral, monitorización y ataques en redes /	Ra-Ma,		978-84-9964-297-0	2014	
Rando González, Enrique.	Hacking con buscadores : Google, Bing & Shodan /	ZeroXword Computing,		978-84-616-7589-0	2014	
González Pérez, Pablo (1976-)	Ethical hacking : teoría y práctica para la realización de u	Zeroxword Computing,		978-84-09-20460-1	2020	
González Pérez, Pablo (1976-)	Pentesting con Kali /	0xWord,		978-84-09-22104-2	2020	