Universidad Zaragoza

Year : 2020/21

30353 - Network and Service Security

Syllabus Information

Academic Year: 2020/21
Subject: 30353 - Network and Service Security
Faculty / School: 110 - Escuela de Ingeniería y Arquitectura
Degree: 438 - Bachelor's Degree in Telecomunications Technology and Services Engineering
ECTS: 6.0
Year: 3
Semester: Second semester
Subject Type: ---
Module: ---

1.General information

1.1.Aims of the course

1.2.Context and importance of this course in the degree

1.3.Recommendations to take this course

2.Learning goals

2.1.Competences

2.2.Learning goals

2.3.Importance of learning goals

3.Assessment (1st and 2nd call)

3.1.Assessment tasks (description of tasks, marking system and assessment criteria)

4.Methodology, learning tasks, syllabus and resources

4.1.Methodological overview

The methodology to be used to achieve the proposed learning results are as follows:

- **Participative Lectures (20 hours).** Presentation by the teacher of the main contents of the subject, combined with the active participation of students. This activity will take place in the classroom. This methodology, supported by the student personal work (M14) is designed to provide them with the theoretical bases of the subject content.
- **Laboratory sessions (40 hours).** The students will have practice sessions for 2 hours each week. This activity will take place at the Laboratory Practices 2.03 (Telematics Laboratory, "Ada Byron" building). The work will be carried out in small groups.
- **Tutoring.**Time for personalized attention to students with the aim of reviewing and discussing the materials and topics presented in both theoretical and practical classes.
- **Evaluation (4 hours).**Set of theoretical tests and/or reporting practices used for the evaluation of student progress. We can find more details in the section of evaluation activities

4.2.Learning tasks

As described in the methodological presentation, the activities are divided into Lectures (20 hours) and laboratory practice (40 hours) in which students can handle security-related software that resolves security scenarios by means of applying the knowledge acquired in lecture sessions.

4.3.Syllabus

The course will address the following topics:

1. Introduction to cybersecurity
2. Practical Cryptography
3. Security in Operational Systems
4. Redundant Systems
5. Malware
6. Botnets: SPAM + Fraud + DDoS
7. Security in the TCP/IP Architecture
8. Security protocols and VPNs
9. Perimetral security
10. Intrusion detection systems
11. Security Information and Event Management (SIEM)

Lab practices:
This activity will be conducted in a computer classroom. It will take in 20 sessions of 2 hours each. Then, students will present the results required for each of the practices.

4.4.Course planning and calendar

Schedule sessions and work presentations

The timing of the subject will be defined by the center in the academic calendar of the corresponding course.

4.5.Bibliography and recommended resources

http://biblos.unizar.es/br/br_citas.php?codigo=30353&year=2019