30353 - Network and Service Security

Información del Plan Docente

Academic Year	2017/18
Faculty / School	110 - Escuela de Ingeniería y Arquitectura
Degree	438 - Bachelor's Degree in Telecomunications Technology and Services Engineering
ECTS	6.0
Year	
Semester	Second semester
Subject Type	
Module	---

1.General information

1.1.Introduction

1.2.Recommendations to take this course

1.3.Context and importance of this course in the degree

1.4.Activities and key dates

2.Learning goals

2.1.Learning goals

2.2.Importance of learning goals

3.Aims of the course and competences

3.1.Aims of the course

3.2.Competences

4.Assessment (1st and 2nd call)

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

5.Methodology, learning tasks, syllabus and resources

5.1.Methodological overview

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

Participative Lectures (30 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.

30353 - Network and Service Security

Classroom practices (15 hours). Exercise solving and practical cases proposed by the teacher, with the possibility of exposing them by students individually or in groups authorized by the teacher. This activity will take place in the classroom, and may require preparatory work by students (M13).
Laboratory sessions (15 hours). The students will have practice sessions 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.

Guided assignments (15 hours). This non-face-to-face activity will allow advancement in all learning outcomes proposed in the topic of security in communications networks. There will be follow-up sessions by the teacher in which each student will present the work done.
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

5.2.Learning tasks

As described in the methodological presentation, the activities are divided into Lectures (30 hours) to be taught in the classroom, classroom practices (15 hours) where scenarios will be resolved for establishing secure communication environments and laboratory practice (15 hours) in which students can handle security related software that resolves security scenarios by means of applying the knowledge acquired in lecture sessions. In addition, there are 15 hours of guided assignments to deepen in topics related to security in communications networks.

5.3.Syllabus

1. CRYPTOLOGY.
1.1. Introduction to Cryptography.
1.1.1. Classical Cryptography.
1.1.2. Modern Cryptography.
1.2. Symmetric Cryptography
1.2.1. Stream Ciphers.
1.2.2. Block Ciphers.
1.3. Asymmetric Cryptography.
1.3.1. Encryption.
1.3.2. Digital Signature.
1.3.3. Public Key Infrastructure.
2. NETWORK&SERVICE SECURITY
2.1 Introduction to Network and Service Security
2.2 Operating System Security
2.3 Redundant Systems
2.4 Malware
2.5 Botnets (SPAM + Fraud + DDoS)
2.6 (Basic) TCP / IP Security
2.7 Anonymity and Identities on the Internet
2.8 Cloud Computing Security
2.9 Perimeter Security (firewalls + iptables)
2.10 Security Protocols and Virtual Private Networks (VPNs)

Lab practices:
This activity will be conducted in a computer classroom. It will taken in 6 sessions of 2 hours each. Then, students will

present the results required for each of the practices.

5.4.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.

5.5.Bibliography and recommended resources

- 1. Kurose, James F.. Computer networking : a top-down approach / James F. Kurose, Keith W. Ross ; international edition adapted by Bhojan Anand . - 4th ed. Boston : Pearson, cop. 2008
- 3. Técnicas criptográficas de protección de datos / Amparo Fúster Sabater...[et al.] . - 2a. ed. rev. y act. Madrid : Ra-ma, D.L. 2000
- 2. Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001
- 4. Caballero Gil, Pino. Introducción a la criptografía / Caballero, Pino Madrid: RA-MA, 2002
- 5. Stallings, William. Cryptography and network security : principles and practice / Williams Stallings . - 3rd ed. Upper Saddle River : Prentice Hall , cop. 2003
- 6. Menezes, Alfred J.. Handbook of applied cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone . - [1st ed.] Boca Raton [etc.] : CRC, cop. 1997
- 7. Schneier, Bruce. Applied cryptography : protocols, algorithms and source code in C / Bruce Schneier New York [etc.] : John Wiley and Sons, cop. 1994