Cybersecurity Systems

Academic Year: (2023 / 2024) **Review date: 16-05-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: PASTRANA PORTILLO, SERGIO

Type: Compulsory ECTS Credits : 6.0

Year : 1 Semester : 1

DESCRIPTION OF CONTENTS: PROGRAMME

1.- Introduction to Cybersecurity
1.1.- Basic concepts

2.- Analysis of systems and networks
2.1.- Introduction to cyberthreats
2.2.- Exploitation vectors
2.3.- Cyberattack techniques
2.4.- Authentication and identification

2.- Cyberdefense in networks
2.1.- Introduction to cyberdefense systems
2.2.- Event monitoring
2.3.- Firewall and network segmentation
2.4.- Intrusion Detection Systems (IDS)
2.5.- Security Information and Event Management (SIEM)

LEARNING ACTIVITIES AND METHODOLOGY

ACTIVITIES

AF1 - Theoretical class. - [30 hours with 100% attendance, 1 ECTS]
AF2 - Practical classes - [3.33 hours with 100% attendance, 0.11 ECTS]
AF3 - Theoretical practical classes - [6 hours with 100% attendance, 0.20 ECTS]
AF4 - Laboratory practices - [9 hours with 100% face-to-face, 0.30 ECTS]
AF5 - Tutorials - [3 hours with 25% attendance, 0.10 ECTS]
AF6 - Group work - [40 hours with 0% attendance, 1.33 ECTS]
AF7 - Individual student work - [84.66 hours with 0% face-to-face, 2.82 ECTS]
AF8 - Midterm and final exams - [4 hours with 100% attendance, 0.13 ECTS]

TEACHING METHODOLOGY

MD1 - Lectures in the teacher's class with computer media support and audiovisual, in which the main concepts of the subject and the bibliography is provided to complement the student learning.
MD2 - Critical reading of texts recommended by the teacher of the subject: Press articles, reports, manuals and / or academic articles, either for further discussion in class, or to expand and consolidate knowledge of the subject.
MD3 - Resolution of practical cases, problems, etc ... raised by the teacher individually or in a group
MD4 - Presentation and discussion in class, under the moderation of the topics related to the content of the subject, as well as cases practical
MD5 - Preparation of works and reports individually or in groups

ASSESSMENT SYSTEM

Continuous assessment:

SE2 [60%] Individual assignments and exams carried out during the course related to the theoretical and laboratory contents

SE3 [40%] Final exam

To pass the course it will be necessary to obtain at least 40% of its weight in the final exam and that the sum between the practical part and the final exam must exceed 50% of the total weight.

Non-continuous evaluation:
The final exam will contain at least 50% of contents related to the laboratory practices

For the extraordinary evaluation, the process will be the same as described above.

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

BASIC BIBLIOGRAPHY

- David Miller Security information and event management (SIEM), McGraw-Hill, 2011

BASIC ELECTRONIC RESOURCES

- National Institute of Standards and Technology (NIST) . Guide to Computer Security Log Management: https://csrc.nist.gov/publications/detail/sp/800-92/final
- Ross Anderson . Security Engineering: https://www.cl.cam.ac.uk/~rja14/book.html