Cybersecurity Systems

Academic Year: (2020 / 2021) **Review date: 23-11-2020**

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

OBJECTIVES

Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.
Ability to state critical opinions and judgements having incomplete or limited information in the field of cyber security. These judgements must take into account include considerations about social and ethical responsibilities.
Discuss in a public audience about their acquired knowledge, and the conclusions from the work. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.
Students should have the learning skills required to continue studying in a autonomous or self-directed way..

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

TEACHING ACTIVITIES
Lectures and oral expositions by the teachers'
Practical classes/Demos
Laboratories
Tutorships
Work in group
Individual group
Final and mid-term exams

ASSESSMENT SYSTEM

Continuous assessment:
- Laboratories (60%)
- Final exam (40%)

To pass the course, students will be required to get a minimum grade in the final exam corresponding to the 40% of its weight. Also, the sum of both the laboratories and final exam marks must be greater than 50% of the final mark.

Non continuous assessment:
It consists of an unique final exam containing at least 50% of contents related to the laboratories

The extraordinary evaluation will follow the similar methodology as explained 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

- Ross Anderson . Security Engineering: https://www.cl.cam.ac.uk/~rja14/book.html