Cybersecurity engineering

Academic Year: (2022 / 2023) **Review date: 30-05-2022**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: ESTEVEZ TAPIADOR, JUAN MANUEL

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Criptography and Information Security (Year 3, Semester 1)
Computer Networks (Year 3, Semester 1)
Operating Systems (Year 2, Semester 2)

SKILLS AND LEARNING OUTCOMES

¿ Know the main threats, risks and vulnerabilities of computer and network systems.
¿ Conceive, design and evaluate solutions that combine cryptographic algorithms, access models and protocols to protect information in a computer system against specific threats.
¿ Know the cybersecurity regulations on privacy and data protection.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to Cybersecurity
1.1. What is cybersecurity?
1.2. The CIA Triad
1.3. Vulnerabilities, Threats, Risks, and Controls
1.4. Adversaries
1.5. Design Principles
1.6. Research Areas in Cybersecurity

2. Authentication
2.1. User Authentication
2.2. Authentication Factors
2.3. Passwords and Password Managers
2.4. Biometric Authentication
2.5. Federated Identity

3. Access Control
3.1. The Protection Problem
3.2. Access Control Models
3.3. Access Control in Linux (I): Credentials and the Permission System:
3.4. Access Control in Linux (II): POSIX ACLs and Capabilities

4. Network Security
4.1. Communication Security
4.2. TCP/IP Security
4.3. Network Discovery and Scanning
4.4. Web Security
4.5. Firewalls
4.6. Intrusion Detection Systems

5. Security Protocols: TLS
5.1. History and Design Goals.
5.2. The Handshake Protocol
5.3. The Record Protocol
5.4. Interception and Certificate Pining

6. Vulnerabilities
6.1. Vulnerability Types
6.2. Numbering (CVE) and Metrics (CVSS)

6.3. Life Cycle of a Vulnerability

7. Malware
7.1. Malicious Code
7.2. Types
7.3. Payloads, Propagation and Activation
7.4. Case Studies

8. Cybersecurity Regulation
8.1. Regulation in the US
8.2. Regulation in the EU
8.3. Privacy Regulation

LEARNING ACTIVITIES AND METHODOLOGY

The teaching methodology includes:
1. Lectures to present the knowledge base that students must acquire. Students will be provided with the lecture notes used in class along with additional documents and basic text references to help in the study of the topics covered. (2 ECTS)
2. Practical lectures, where the students will have to solve exercises and quizzes. (1 ECTS)
3. Discussion of real cases to illustrate concepts and techniques introduced during the lectures. (1 ECTS)
4. Lab sessions in computer labs, where the students will learn techniques and develop skills in the use of cybersecurity tools, including binary analysis, distributed systems security and network security. (2 ECTS)

ASSESSMENT SYSTEM

The final mark will depend on the following criteria:
(a) Lab assignments: 40%. These lab exercises are compulsory and will be marked by grading the associated deliverables and, in some cases, oral presentation of the results.
(b) Final exam: 60%. Sitting the final exam is compulsory. The student must get at least 50% of the maximum mark to pass the course.

There will be a special examination session where the student who has followed the continuous assessment scheme described above (lab sessions) will be able to seat an exam. In such a case, the final mark will be computed using the scheme described above. Alternatively, the student can choose to seat just a final exam. In this case, the final mark will be that of the final exam.

In all other circumstances not covered above, the procedure established by the University on the 31st of May, 2011 will be followed.

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

BASIC BIBLIOGRAPHY

- Anderson, Ross SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTRED SISTEMS (2nd edition), Wiley, 2008
- Pfleeger, Charles. Pfleeger, Shari L SECURITY IN COMPUTING (4ª edition), Prentice Hall, 2007

ADDITIONAL BIBLIOGRAPHY

- Vacca, John R. (Editor). COMPUTER AND INFORMATION SECURITY HANDBOOK., Elsevier (The Morgan Kaufmann Series in Computer Security)., 2009.

BASIC ELECTRONIC RESOURCES

- ENISA . Publications: http://www.enisa.europa.eu
- INCIBE . OSI/CERTSI: https//www.incibe.es
- NIST . Special Publications (NIST-SP): http://www.nist.gov/publication-portal.cfm