Cybersecurity engineering

Academic Year: (2022 / 2023) **Review date: 14-06-2022**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: ESTEVEZ TAPIADOR, JUAN MANUEL

Type: Compulsory ECTS Credits : 6.0

Year : 5 Semester : 1

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

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