Course Unit	Cybersecurity			Field of study	Computer Engineering		
Bachelor in	Informatics Engineering			School	School of Technology and Management		
Academic Year	2022/2023	Year of study	3	Level	1-3	ECTS credits	6.0
Type	Semestral	Semester	2	Code	9119-706-3201-00-22		

Workload (hours)	162	Contact hours	T -	TP 60	PL -	TC -	S -	E -	OT -	O -

T - Lectures; TP - Lectures and problem-solving; PL - Problem-solving, project or laboratory; TC - Fieldwork; S - Seminar; E - Placement; OT - Tutorial; O - Other

Name(s) of lecturer(s): Tiago Miguel Ferreira Guimaraes Pedrosa, Miguel de Lacerda Pereira, Rui Alexandre Coelho Alves

Learning outcomes and competences

At the end of the course unit the learner is expected to be able to:
1. Recognize the importance of security issues in computer systems and networks;
2. Identify the main types of vulnerabilities, attack vectors against networks and systems, and solutions to minimize them;
3. Install, configure and manage security solutions and mechanisms;
4. Harden Systems and Networks;
5. Conduct security audits and intrusion tests on systems and networks.

Prerequisites

Before the course unit the learner is expected to be able to:
Demonstrate basic knowledge of systems and networks.

Course contents

Fundamentals of system and network security. Concepts of cryptography. Vulnerabilities and attacks. Mechanisms for control, containment, detection and prevention. Industrial cybersecurity. Systems and networks hardening. Security audit and penetration testing.

Course contents (extended version)

1. Fundamentals of security in computer systems and networks
2. Introduction to cryptography
3. Vulnerabilities and Attack Vectors
4. Control, Containment, Detection and Prevention Mechanisms and Solutions
5. System and Network Hardening
6. Security audit and penetration testing

Recommended reading

1. W. Stallings, "Network Security Essentials: Applications and Standards, 6th edition", Pearson, 2021
2. W. Stallings, "Cryptography And Network Security, 7Th Edition ", Pearson, 2017
3. M. Gregg, D. Kim, "Inside Network Security Assessment", Sams, 2006
4. A. Zúquete, "Segurança em Redes Informáticas - 6 ed", FCA, 2021
5. V. Velu, "Mastering Kali Linux for Advanced Penetration Testing: Become a cybersecurity ethical hacking expert using Metasploit, Nmap, Wireshark, and Burp Suite, 4th Edition", Packt Publishing, 2022

Teaching and learning methods

The unit will be taught using a combination of lectures, practical classes and the execution of transversal projects for the application of the security concepts. The unit documentation will be available through e-learning facilities, with support via slack/discord.

Assessment methods

1. Final, Supplementary - (Regular, Student Worker) (Final, Supplementary)
   - Projects - 60% (Two projects, each 30%.)
   - Practical Work - 20% (Practical tasks.)
   - Final Written Exam - 20%
2. Special - (Regular, Student Worker) (Special)
   - Projects - 70% (Two projects, each 35%.)
   - Final Written Exam - 30%

Language of instruction

1. Portuguese
2. English

Electronic validation

Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	Luísa Maria Garcia Jorge	José Carlos Rufino Amaro
07-03-2023	17-03-2023	23-03-2023	25-03-2023