COURSE DESCRIPTION – ACADEMIC YEAR 2024/2025

Course title	**Software and System Security**
Course code	76097
Scientific sector	ING-INF/05
Degree	Master in Software Engineering (LM-18)
Semester	2
Year	1
Credits	6
Modular	No

Total lecturing hours	40
Total exercise hours	20
Attendance	Not compulsory, but recommended especially for the labs. Non-attending students must contact the lecturer at the start of the course to agree on the modalities of the independent study.
Prerequisites	Students are expected to have software engineering foundation and be familiar with the basics of information security. These prerequisites are normally covered in any Bachelors in Computer Science.
Course page	https://ole.unibz.it/

Specific educational objectives	The course belongs to the type "caratterizzanti – discipline informatiche". The aim of the course is providing students with a comprehensive understanding of the principles, techniques, and best practices related to securing software systems and computer systems. At the end of the course, the students will: • Understand fundamental computer security principles, including confidentiality, integrity, and availability • Understand software security practices, including secure coding and software development methodologies. • Understand network security principles, including firewalls, intrusion detection, and secure communication protocols. • Understand social engineering attacks and techniques used by adversaries • Learn common system vulnerabilities and potential attack vectors and methods to detect them • Learn incident response strategies and recovery techniques. • Learn about security auditing, monitoring, and incident response planning

Lecturer	Barbara Russo
Contact LA	Via Bruno Buozzi 1, Room B1.4.20, barbara.russo@unibz.it, 0471-016170
Scientific sector of lecturer	INF-01
Teaching language	English
Office hours	During the lecture time span, TBD, arrange beforehand by email, POS-115, Piazza Domenicani 3
Lecturing Assistant (if any)	*TBD*

Contact LA	*office, e-mail, phone*
Office hours LA	--
List of topics	• Computer Security Technology and Principles • Data security • Software and Network Security and Trusted Systems • Social security • System Vulnerabilities and Attacks • Security Management
Teaching format	Frontal lectures and lab assignements

Learning outcomes	**Knowledge and Understanding** • D1.1 possess solid knowledge of both the fundamentals and the application aspects of the various fundamental areas of computer science; • D1.4 have an in-depth knowledge of the principles, structures and use of processing systems for the automation of software systems **Applying knowledge and understanding** • D2.1 know how to apply the fundamentals of empirical analysis of ICT data for the construction of mathematical models for the evaluation and prediction of characteristics of applications and software systems; **Making judgments** • D3.2 ability to plan and re-plan a technical project activity and to carry it out within the defined deadlines and objectives; **Communication skills** • D4.1 ability to present the contents of a scientific/technical report in a set time in front of an audience, including non-specialists; • D4.4 ability to prepare and deliver presentations with technical content in English; **Learning skills** • D5.2 ability to independently keep up to date with developments in the most important fields of information technology;

Assessment	Written exam and lab work: written exam with verification questions and lab assignments
Assessment language	English
Assessment typology	Non-Monocratic
Evaluation criteria and criteria for awarding marks	*Final grade: 5*0% project work and 50% written exam. *Lab assessment must be positive (i.e., 18 or higher) to access the written exam.* Relevant for the assessment: Lab assessment: ability to apply in autonomy and develop further instruments introduced during the lectures/labs and needed to accomplish tasks and perform little studies with data. Ability to report in a professional manner also using the appropriate terminology and concepts of the course.

	Written exam: being able to master the terminology of the course; being able to evaluate tools and techniques and their technical details for specific domain of use; being able to solve exercises or summarize theoretical concepts.

Required readings	Ross Anderson, Security Engineering, Editore: Wiley, ISBN: 0-471-38922-6 http://www.cl.cam.ac.uk/~rja14/book.html Paul C. van Oorschot Computer Security and the Internet: Tools and Jewels https://people.scs.carleton.ca/~paulv/toolsjewels.html William Stallings Lawrie Brown Computer Security Principles and Practice, 5th edition Published by Pearson (July 28, 2023) © 2024 Dafydd Stuttard, Marcus Pinto The web application hacker's handbook: discovering and exploiting security flaws. John Wiley & Sons, Inc., USA. Dieter Gollmann Computer Security John Wiley & Sons Inc Subject Librarian: David Gebhardi, David.Gebhardi@unibz.it
Supplementary readings	Supplementary readings will be given during the lectures
Software used	Python, Open Source software or fortify suite if available