SYLLABUS

1. Data about the program of study

1.1	Institution	Technical University of Cluj-Napoca
1.2	Faculty	Automation and Computer Science
1.3	Department	Computer Science
1.4	Field of study	Computer Science and Information Technology
1.5	Cycle of study	Master of Science
1.6	Program of study / Qualification	Cybersecurity Engineering / Master
1.7	Form of education	Full time
1.8	Subject code	10.

2. Data about the subject

2.1	Subject name			***Research Activity 2***		
2.2	Course responsible/lecturer			N/A		
2.3	Teachers in charge of applications			Conf. dr. ing. Adrian COLEȘA - adrian.colesa@cs.utcluj.ro		
2.4 Year of study	I	2.5 Semester	2	2.6 Type of assessment (E - exam, C - colloquium, V - verification)		V
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary					DS
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)					DI

3. Estimated total time

3.1 Number of hours per week	14	of which	3.2 Course	0	3.3 Seminar	0	3.3 Laboratory	0	3.3 Project	14
3.4 Total hours in the curriculum	196	of which	3.5 Course	0	3.6 Seminar	0	3.6 Laboratory	0	3.6 Project	196

3.7 Individual study:	
(a) Manual, lecture material and notes, bibliography	0
(b) Supplementary study in the library, online and in the field	25
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays	0
(d) Tutoring	0
(e) Exams and tests	4
(f) Other activities	0

3.8 Total hours of individual study (sum (3.7(a)...3.7(f)))	29
3.9 Total hours per semester (3.4+3.8)	225
3.10 Number of credit points	9

4. Pre-requisites (where appropriate)

4.1	Curriculum	Research Activity 1
4.2	Competence	Competences of subjects mentioned at 4.1

5. Requirements (where appropriate)

5.1	For the course	N/A
5.2	For the applications	Hardware and software specific to dissertation theme

6. Specific competences

Professional competences	**C2. Investigate and analyze cyber-criminality actions and malware using advanced methods such as reverse engineering and behavior monitoring.** • **C2.1.** Advanced knowledge of classifications and characteristics of different cybersecurity attacks and malware. • **C2.2.** Be able to analyze and understand new kinds of malware, the new techniques they use to attack, gain persistence, escalate privileges etc., and be able to compare them with known attack techniques. • **C2.3.** Capability to identify malicious entities and activities, having no inside visibility on them (using black-box strategy). • **C2.4.** Capability to identify and assess theoretical and practical limitations of existing automatic malware analysis tools and propose improvements, where and if possible. • **C2.5.** Capability to derive new classes of attacks and exploitation techniques, supposed to be used by new malware, and propose the appropriate methods to identify and classify them correctly. **C3. Analyze and evaluate the security characteristics of computing system. Identify the misconfigurations and software vulnerabilities.** • **C3.1.** Theoretical and practical knowledge of different cases of computing system misconfiguration and misusage that expose them to cybersecurity attacks, and of different types of software vulnerabilities and possible cybersecurity attacks. • **C3.2.** Be able to analyze and understand new kinds of software and communication protocols, in order to identify new possible cybersecurity threats, vulnerabilities, and risks. Be able to use commonly used databases of reported vulnerabilities and attacks in the process of assessing the cybersecurity of a new computing system. • **C3.3.** Capability to make cybersecurity assessments and identify possible attack surface of unknown computing systems, networks, or software applications. • **C3.4.** Capability to identify and assess theoretical and practical limitations of existing automatic vulnerability detection tools and propose possible combinations of such tools for improved results, where and if possible. • **C3.5.** Capability to propose new vulnerability identification, analysis, and classification, methods. Capability to propose solutions against exploitation techniques of such vulnerabilities. **C4. Design and develop highly secure software, security solutions and tools.** • **C4.1.** Knowledge of basic concepts and principles of secure software development and evaluation. Knowledge of common types of security software and tools. Knowledge of different operating system architectures, hardware and software infrastructures and frameworks needed to develop effective security solutions. • **C4.2.** Be able to identify new situations and scenarios when it is needed to develop a new cybersecurity solution or use an existing one. Be able to analyze proposed cybersecurity solutions and compare them with existing ones. • **C4.3.** Capability to develop complex secure software, complying with recommended good practices of built-in security and secure coding. Capability to develop software tools used for cybersecurity pentesting and assessment. • **C4.4.** Capability to assess complex software projects and identify their cybersecurity vulnerabilities and flaws, regarding their design, implementation, or testing, and propose improved development methods from the cybersecurity perspective. • **C4.5.** Capability to develop software modules and tools that could provide a high degree of cybersecurity. Capability to propose new methods to assess the cybersecurity of computing systems and devices and ways to improve it.
Cross competences	N/A

7. Discipline objectives (as results from the *key competences gained*)

7.1	General objective	Gain the ability and skills to do research, design, development, and assessment work in the cybersecurity field.
7.2	Specific objectives	1. Define objectives for dissertation work and thesis. 2. Have detailed knowledge about the state-of-the-art of the dissertation thesis'

		domain and theme. 3. Identify and define a clear research direction and open problems for the dissertation work. 4. Propose possible solutions for the identified problems.

8. Contents

8.1. Lecture (syllabus)	Number of hours	Teaching methods	Notes
N/A	N/A	N/A	N/A
Bibliography N/A			
8.2. Seminar / Laboratory / Project	Number of hours	Teaching methods	Notes
1. Critical analysis of existing solutions to problems and challenges addressed by chosen dissertation theme and problems. 2. Identify and define investigation plans and directions and possible solutions. 3. Estimate the effort and resources needed to implement and validate the proposed solutions. 4. Define a time schedule regarding the theoretical and practical research activity, in accordance with the proposed solutions and estimated effort. 5. Design the main architecture and components of the solutions and system aimed to be developed. 6. Design the main components and algorithms of the solutions and system aimed to be developed. 7. Perform experiments, tests and validations. 8. Write a technical report describing research activity performed and obtained results.	14	Cooperation between dissertation supervisor and student	
Bibliography Established by each supervisor for students she/he coordinates, specific to chosen dissertation themes.			

9. Bridging course contents with the expectations of the representatives of the community, professional associations, and employers in the field

It is performed by periodic talks with important cybersecurity industry representatives.

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Project	Based on the contents and relevance of the written technical report	Oral presentation Technical report's quality	60% 40%
Minimum standard of performance Identify at least one open problem regarding the chosen dissertation theme, propose at least one solution to the identified problem, establish working plan and time scheduler, design the aimed system / solution architecture, write a minimum 5 page technical report.			

Date of filling in		Title Surname Name	Signature
	Teachers in charge of application	Conf. dr. ing. Adrian COLEȘA	

Date of approval in the Computer Science Department 20.02.2024	Head of department Prof.dr.ing. Rodica Potolea
Date of approval in the faculty of Automation and Computer Science 22.02.2024	Dean Prof.dr.ing. Mihaela Dinsoreanu