SYLLABUS

1. Data about the program of study

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

2. Data about the subject

2.1 Subject name	***Research Activity 3***			Subject code	**16**
2.2 Course responsible / lecturer	N/A				
2.3 Teachers in charge of seminars / Laboratory / project	Assoc. prof. dr. eng. Colesa Adrian - adrian.colesa@cs.utcluj.ro				
2.4 Year of study	II	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	V
2.7 Subject category	Formative category: DF – fundamental, DS – speciality, DC – complementary				DS
	Optionality: DOB – mandatory, DOP – optional (alternative), DFA – optional (free choice)				DOB

3. Estimated total time

3.1 Number of hours per week	14	of which:	Course	-	Seminars	-	Laboratory	-	Project	14
3.2 Number of hours per semester	196	of which:	Course	-	Seminars	-	Laboratory	-	Project	196
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										-
(b) Supplementary study in the library, online and in the field										-
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										3
(d) Tutoring										-
(e) Exams and tests										1
(f) Other activities:										-

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	4
3.5 Total hours per semester (3.2+3.4)	220
3.6 Number of credit points	8

4. Pre-requisites (where appropriate)

4.1 Curriculum	Research Activity 1 and 2
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 competence

6.1 Professional competences	• perform ICT security testing • perform data analysis • identify ICT security risks • perform risk analysis • ensure information privacy • monitor developments in field of expertise • keep up with the latest information systems solutions • execute ICT audits
6.2 Cross competences	• develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded

7. Expected Learning Outcomes

Knowledge	• ICT security standards • security engineering • cyber security • cyber attack counter-measures • information confidentiality • information security strategy • computer forensics • ethical hacking principles • risk management • assessment of risks and threats • attack vectors • security threats • ICT infrastructure • ICT performance analysis methods
Skills	• analyse ICT systems • define technical requirements • identify ICT security risks and weaknesses • perform ICT security testing • perform risk analysis • collect cyber defence data • perform scientific research • report test findings and give live presentations • solve ICT system problems • address problems critically • assess ICT knowledge • execute ICT audits • implement ICT security policies • interpret technical texts
Responsibilities and autonomy	• develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	Gain the ability and skills to do research, design, development, and assessment work in the cybersecurity field.
8.2 Specific objectives	1. Assess the proposed solutions and bring needed improvements. 2. Make proposed solutions functional in real-life scenarios.

	3. Disseminate obtained results (e.g. publish a paper).

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
N/A	N/A	N/A	N/A
Bibliography N/A			
9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Keep up to date to the state-of-the art of the field of chosen dissertation theme and problems.	14	Cooperation between dissertation supervisor and student.	
Elaborate the detailed design of main components of the proposed solutions and system aimed to be developed.			
Implement and assess a prototype of the system / app that validates proposed solutions and show their limitations.			
Propose possible improvements.			
Write a technical report describing research activity performed and obtained results.			
Write a scientific paper and submit it to a conference or journal in the cybersecurity field.			
Bibliography Established by each supervisor for students she/he coordinates, specific to chosen dissertation themes.			

10. 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.

11. 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 presentations *(continuous assessment)* Technical report's quality *(summative assessment)*	60% 40%
Minimum standard of performance: Implement and asses at least one solution from those proposed, write a minimum 5 page technical report.			

Date of filling in 29.04.2026	**Responsible**	**Title First name Last name**	**Signature**
	Applications	Assoc.prof.dr.eng. Adrian COLEȘA	

Date of approval in the department	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council	Dean, Prof.dr.eng. Vlad Mureșan