COURSE SYLLABUS

Academic year 2025 - 2026

1. Programme Information

1.1. Higher education institution	Lucian Blaga University of Sibiu
1.2. Faculty	Faculty of Science
1.3. Department	Mathematics and Informatics
1.4. Field of study	Informatics
1.5. Level of study[1]	Master
1.6. Programme of study/qualification	Cybersecurity

2. Course Information

2.1. Name of course	Vulnerability analysis of computer systems			Code	FSTI.MAI.CS.M.SA.2.2020.E-6.4
2.2. Course coordinator	Lecturer PhD. Oana-Adriana Ticleanu				
2.3. Seminar/laboratory coordinator	Lecturer PhD. Oana-Adriana Ticleanu				
2.4. Year of study[2]	1	2.5. Semester[3]	2	2.6. Evaluation form[4]	E
2.7. Course type[5]	R	2.8. The formative category of the course[6]			F

3. Estimated Total Time

3.1. Course Extension within the Curriculum – Number of Hours per Week				
3.1.a. Lecture	3.1.b. Seminar	3.1.c. Laboratory	3.1.d. Project	Total
2		2		**4**
3.2. Course Extension within the Curriculum – Total Number of Hours within the Curriculum				
3.2.a. Lecture	3.2.b. Seminar	3.2.c. Laboratory	3.2.d. Project	Total[7]
28		28		**56**

Time Distribution for Individual Study[8]	**Hours**
Learning by using course materials, references and personal notes	27
Additional learning by using library facilities, electronic databases and on-site information	27
Preparing seminars / laboratories, homework, portfolios and essays	29
Tutorial activities[9]	7
Exams[10]	4
3.3. Total Individual Study Hours[11] *(NOSI$_{sem}$)*	**94**
3.4. Total Hours in the Curriculum (*NOAD$_{sem}$*)	**56**
3.5. Total Hours per Semester[12] (*NOAD$_{sem}$ + NOSI$_{sem}$*)	**150**
3.6. No. of Hours / ECTS	**25**
3.7. Number of credits[13]	**6**

4. Prerequisites (if needed)

4.1. Courses that must be successfully completed first (from the curriculum)[14]	Cybersecurity Introduction
4.2. Competencies	-

5. Conditions (where applicable)

5.1. For course/lectures[15]	Classroom, equipped with blackboard, computer, video projector and software
5.2. For practical activities (lab/sem/pr/app) [16]	Laboratory room equipped with computers

6. Learning Outcomes [17]

Number of credits assigned to the discipline: 6				
Learning outcomes				Credit distribution by learning outcomes
Nr. crt.	Knowledge	Skills	Responsibility and autonomy	
LO 1	The student defines and classifies vulnerability analysis techniques and categories of information confidentiality protection systems.	The student analyzes and compares vulnerability models applied to personal and SOHO systems.	The student critically evaluates and reports identified vulnerabilities, demonstrating autonomy in choosing methodologies.	2
LO 2	The student describes vulnerability analysis models for computing systems of private institutions not integrated into networks.	The student applies testing methods and produces vulnerability assessment reports for such systems.	The student assumes responsibility for accurate documentation and proposes remediation solutions.	1.5
LO 3	The student explains the specifics of vulnerability analysis for systems integrated into local and global networks.	The student simulates attack scenarios and assesses risks for interconnected systems.	The student demonstrates autonomy in using specialized tools and complies with ethical and legal standards.	1.5
LO 4	The student understands the particularities of vulnerability models for computing systems of government institutions.	The student develops and applies analysis models for such systems, considering national security constraints.	The student shows high responsibility in handling sensitive information and adopts a professional ethical conduct.	1

7. Course objectives (resulted from developed competencies)

7.1. Main course objective	Acquiring the necessary knowledge in order to detect the vulnerabilities of the hardware and software systems used in the confidentiality of information.
7.2. Specific course objectives	Understanding the rules for analyzing vulnerability patterns of information protection systems and risk mitigation techniques.

8. Content

8.1. Lectures[18]	**Teaching methods**[19]	**Hours**

Definition of the techniques for analyzing the vulnerabilities of computer system protection systems and the categories of information confidentiality systems.	Lecture, use of video projector, discussions with students	4
Vulnerability analysis models of personal computing systems	Lecture, use of video projector, discussions with students	4
Vulnerability analysis models of SOHO systems	Lecture, use of video projector, discussions with students	4
Vulnerability analysis models of computing systems of private institutions for the case of models not integrated into networks.	Lecture, use of video projector, discussions with students	4
Vulnerability analysis models of computing systems of private institutions for the case of models integrated in local networks.	Lecture, use of video projector, discussions with students	4
Vulnerability analysis models of computing systems of private institutions for the case of models integrated in global networks.	Lecture, use of video projector, discussions with students	4
Vulnerability analysis models of computing systems of government institutions	Lecture, use of video projector, discussions with students	4
	Total lecture hours:	**28**

8.2. Practical activities (8.2.a. Seminar[20]/ 8.2.b. Laboratory[21]/ 8.2.c. Project[22])	**Teaching methods**	**Hours**
Vulnerability analysis software for computer protection systems. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
Vulnerability analysis software for personal computer systems. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
SOHO system vulnerability analysis software. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
Software for analyzing the vulnerabilities of the computing systems of private institutions for the case of models not integrated in the networks. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
Software for analyzing the vulnerabilities of computing systems of private institutions for the case of models integrated in local networks. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
Software for analyzing the vulnerabilities of computing systems of private institutions for the case of models integrated in global networks. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
Software for analyzing the vulnerabilities of the computing systems of governmental institutions. Installation, configuration, periodic check.	Use of video projector, discussions with students	4
	Total seminar/laboratory hours:	28

9. Bibliography

9.1. Recommended Bibliography	1. M. Lehto, P. Neittaanmaki, Cyber Security - Analytics, Technology and Automation, Springer 2015 2. S. Guo, D. Zeng, Cyber-Physical Systems - Architecture, Security and Application, Springer 2019
9.2. Additional Bibliography	1. D. Atkins, T. Sheldon, Hacking-Firewalls And Networks How To Hack Into Remote Computers 2. E. Nuwere, D. Chanoff, Hacker Cracker, PerfectBound 2009 3. R. Wobst, Cryptology Unlocked, Wiley 2007

10. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program[23]

It is done through regular contacts with the representatives of the companies. Cybersecurity topic is actual and is of great interest in existing software companies on the local, national and global market.

11. Evaluation

Activity Type	11.1 Evaluation Criteria	11.2 Evaluation Methods		11.3 Percentage in the Final Grade	Obs.[24]
11.4a Exam / Colloquy	• Theoretical and practical knowledge acquired (quantity, correctness, accuracy)	Tests during the semester[25]:	%	50% (minimum 5)	CEF
		Homework:	%		
		Other activities[26]:	%		
		Final evaluation:	50%		
11.4b Seminar	• Frequency/relevance of participation or responses	Evidence of participation, portfolio of papers (reports, scientific summaries)		5% (minimum 5)	nCPE
11.4c Laboratory	• Knowledge of the equipment, how to use specific tools; evaluation of tools, processing and interpretation of results	• Written questionnaire • Oral response • Laboratory notebook, experimental works, reports, etc. • Practical demonstration		5% (minimum 5)	nCPE
11.4d Project	• The quality of the project, the correctness of the project documentation, the appropriate justification of the chosen solutions	• Self-evaluation, project presentation • Critical evaluation of a project		40% (minimum 5)	nCPE
11.5 Minimum performance standard[27] The student is able to define the basic concepts and techniques of vulnerability analysis**,** apply at least one analysis model to a simple computing system (e.g., personal or SOHO), and produce a basic report highlighting identified vulnerabilities and possible remediation measures.					

The Course Syllabus will encompass components adapted to persons with special educational needs (SEN – people with disabilities and people with high potential), depending on their type and degree, at the level of all curricular elements (skills, objectives, contents, teaching methods, alternative assessment), in order to ensure fair opportunities in the academic training of all students, paying close attention to individual learning needs.

Filling Date: |_1_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

Department Acceptance Date: |_3_|_0_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

	Academic Rank, Title, First Name, Last Name	**Signature**
Course Teacher	Lecturer PhD. Oana-Adriana Ticleanu	
Study Program Coordinator	Associated Professor PhD. Nicolae Constantinescu	
Department Head	Professor PhD. Mugur Acu	

[1] *Bachelor / Master*
[2] *1-4 for bachelor, 1-2 for master*
[3] *1-8 for bachelor, 1-3 for master*
[4] *Exam, colloquium or VP A/R - from the curriculum*
[5] *Course type: R = Compulsory course; E = Elective course; O = Optional course*
[6] *Formative category: S = Specialty; F = Fundamental; C = Complementary; I = Fully assisted; P = Partially assisted; N = Unassisted*
[7] *Equal to 14 weeks x number of hours from point 3.1 (similar to 3.2.a.b.c.)*
[8] *The following lines refer to individual study; the total is completed at point 3.37.*
[9] *Between 7 and 14 hours*
[10] *Between 2 and 6 hours*
[11] *The sum of the values from the previous lines, which refer to individual study.*
[12] *The sum (3.5.) between the number of hours of direct teaching activity (NOAD) and the number of hours of individual study (NOSI) must be equal to the number of credits assigned to the discipline (point 3.7) x no. hours per credit (3.6.)*
[13] *The credit number is computed according to the following formula, being rounded to whole neighbouring values (either by subtraction or addition*

$$No.credits = \frac{NOCpSpD \times C_C + NOApSpD \times C_A}{TOCpSdP \times C_C + TOApSdP \times C_A} \times 30\ credits$$

Where:

- NOCpSpD = Number of lecture hours / week / discipline for which the credits are calculated
- NOApSpD = Number of application hours (sem./lab./pro.) / week / discipline for which the credits are calculated
- TOCpSdP = Total number of course hours / week in the Curriculum
- TOApSdP = Total number of application hours (sem./lab./pro.) / week in the Curriculum
- C_C/C_A = Course coefficients / applications calculated according to the table

Coefficients	**Course**	**Applications (S/L/P)**
Bachelor	2	1
Master	2,5	1,5
Bachelor - foreign language	2,5	1,25

[14] *The courses that should have been previously completed or equivalent will be mentioned*
[15] *Board, video projector, flipchart, specific teaching materials, online platforms, etc.*
[16] *Computing technology, software packages, experimental stands, online platforms, etc.*
[17] *Competences from the Grids related to the description of the study program, adapted to the specifics of the discipline*
[18] *Chapter and paragraph titles*
[19] *Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)*
[20] *Discussions, debates, presentations and/or analyses of papers, solving exercises and problems*
[21] *Practical demonstration, exercise, experiment*
[22] *Case study, demonstration, exercise, error analysis, etc.*
[23] *The relationship with other disciplines, the usefulness of the discipline on the labour market*
[24] *CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable*
[25] *The number of tests and the weeks in which they will be taken will be specified*
[26] *Scientific circles, professional competitions, etc.*
[27] *The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable*