COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
METHODS OF ETHICAL HACKINGS	

Academic staff	Core academic unit(s)
Coordinating: teach. assist. Paulius Danielius **Other:**	Institute of Social Sciences and Applied Informatics Kaunas Faculty 8 Muitines st, LT-44280 Kaunas

Study cycle	Type of the course unit
First	Compulsory

Mode of delivery	Semester or period when it is delivered	Language of instruction
Face-to-face	4th semester	Lithuanian/English

Requisites	
Prerequisites: Fundamentals of Information System Security, Operating Systems and Their Security, Data Security and Cryptography	**Co-requisites (if relevant):**

Number of ECTS credits allocated	Student's workload (total)	Contact hours	Individual work
5	130	52	78

Purpose of the course unit		
Learning outcomes of the course unit	**Teaching and learning methods**	**Assessment methods**
Students will be able to understand the methods and objectives of ethical hacking and security- testing Strategies; students will know the limits and capabilities of method application.	Lectures, practical assignments, independent work, active learning methods (group discussion, case study)	Laboratory classes. Final examination
Students will be able to remotely identify systems, apply vulnerability search tools; apply typical attack methods and strategies, choose security measures against typical attacks.		
Students will be ready to take certification as ethical hackers		

Content	Contact hours							Individual work: time and assignments	
	Lectures	Tutorials	Seminars	Workshops	Laboratory work	Internship	**Contact hours, total**	**Individual work**	**Tasks for individual work**
1. Introduction to Hacking - Ethical Hacking: A Beginner's Guide.	2			2			**4**	**5**	Analysis of literature
2. The Operations Management and Workplace Preparation	2			4			**6**	**5**	Practical preparation of own workplace
3. The Kill Chain in Cyberspace.	2			2			**4**	**5**	Practical assignments
4. Obtaining the information.	1			2			**3**	**6**	Analysis of literature. Practical assignments
5. The scanning overviews. Network scanning.	1			2			**3**	**6**	Analysis of literature
6. The scanning techniques. Network scanning.	1			4			**5**	**6**	Practical assignments
7. Vulnerability scanning. Network scanning and vulnerability scanning.	1			4			**5**	**6**	Analysis of literature
8. Vulnerability tools.	1			4			**5**	**6**	Analysis of literature
9. Auditing of passwords.	1			2			**3**	**10**	Analysis of literature
10. Shell: Meterpreter.	1			2			**3**	**8**	Analysis of literature
11. Network flows in network behavior.	1			2			**3**	**5**	Practical assignments
12. OSSTMM and case analysis.	2			2			**4**	**10**	Analysis of literature
Consultation		2					**2**		
Final examination							**2**		
TOTAL	**16**	**2**		**32**			**52**	**78**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Practical assignments	60 (4 x 15)	During semester	Four practical work defenses, during which completed tasks are checked and additional questions are asked.
Final examination	40	During Session	The exam covers the theoretical and practical material of the entire subject and is graded on a 10-point scale according to VU assessment criteria. The exam format is a mixed test, which includes questions with one correct answer, questions with several correct answers, and questions requiring a "yes" or "no" answer.

Author (-s)	Publishing year	Title	Issue of a periodical or volume of a publication	Publishing house or web link
Required reading				
P. Danielius	2025	Lectures material		https://emokymai.vu.lt/?lang=en
Peter Kim	2014	The Hacker Playbook 2: Practical Guide To Penetration Testing		CreateSpace Independent Publishing Platform
Pat Engebretson	2013	Basics of Hacking & Penetration Testing	2nd Edition	Syngress.
Justin Hutchens	2014	Kali Linux Network Scanning Cookbook		PACKT Publishing
Recommended reading				
Michael E. Whitman, Herbert J. Mattord	2011	Hands-on Information security Lab Manual	3th edition	Course Technology, Cengage Learning.
Pete Herzog	2010	The Open Source Security Testing Methodology Manual	3th edition	ISECOM