COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
METHODS OF ETHICAL HACKINGS	

Academic staff	Core academic unit(s)
Coordinating: jun. 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		
Develop the ability to understand and apply modern methods of hacking into an organization's network, use them to perform a security check of the organization's network, and, based on the results obtained, be able to select relevant security solutions.		
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 and apply vulnerability search tools; Students will be able to apply typical attack methods and strategies and 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. Modern Ethical Hacking. Legal and ethical frameworks. The Operations Management and Workplace Preparation	2			4			**6**	**5**	Analysis of literature Practical preparation of own workplace
2. Reconnaissance & MITRE ATT&CK. Active and passive scanning. Threat modeling using the MITRE ATT&CK framework.	2			2			**4**	**5**	Practical assignments
3. Vulnerability Management. Risk assessment based on CVSS 4.0. EPSS metrics and vulnerability prioritization.	2			8			**10**	**12**	Analysis of literature Practical assignments
4. Exploitation & Evasion Techniques. Advanced Metasploit usage. EDR/AV evasion basics and post-exploitation techniques.	2			6			**8**	**18**	Analysis of literature Practical assignments
5. Identity & Access Auditing. MFA bypass techniques (AiTM). Modern authentication (OAuth2, FIDO2) and Active Directory security.	2			4			**6**	**16**	Analysis of literature Practical assignments
6. Web & API Security. OWASP Top 10 analysis. Identification and testing of API logic vulnerabilities (BOLA/BFLA).	2			4			**4**	**6**	Analysis of literature
7. Cloud & Infrastructure Attacks. Azure/AWS configuration security. Container (Docker, Kubernetes) security vulnerabilities.	2			2			**6**	**6**	Analysis of literature
8. Reporting & Remediation. Presenting results to business. Incident response and collaboration with defenders (Purple Teaming).	2			2			**4**	**10**	Analysis of literature Practical assignments
Consultation		2					**2**		
Final examination							**2**		
TOTAL	**16**	**2**		**32**			**52**	**78**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Practical assignments	50	2-16th week	Practical work defenses, during which completed tasks are evaluated and additional questions are provided.
Research Project and Presentation	10	14-15th week	Analysis of a selected modern cybersecurity incident or technological threat by applying theoretical knowledge gained during the course. Oral presentation with visual aids, focusing on technical lessons learned and business recommendations.
Final examination	40	During the 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.

IMPORTANT! A student who (1) throughout the semester consistently fails to demonstrate progress in achieving the expected learning outcomes of a subject (module) during the practical classes (seminars, exercises, laboratory work, etc.) and (2) fails to complete all interim assessment requirements and tasks within the time specified in the course description, is not allowed to participate in the examination session.

Author (-s)	Publishing year	Title	Issue of a periodical or volume of a publication	Publishing house or web link
Required reading				
P. Danielius	2026	Lectures material		https://emokymai.vu.lt/?lang=en
Wilhelm Thomas	2025	Professional Penetration Testing: Creating and Learning in a Hacking Lab.	3rd edition	Elsevier Inc.
Estrin Eyal	2022	Cloud Security Handbook : Find out How to Effectively Secure Cloud Environments Using AWS, Azure, and GCP		Packt Publishing
Rawal Bharat S, Peter Alexender, Manogaran, Gunasekaran	2022	Cybersecurity and Identity Access Management		Springer
Velu Vijay Kumar	2022	Mastering Kali Linux for Advanced Penetration Testing: Become a Cybersecurity Ethical Hacking Expert Using Metasploit, Nmap, Wireshark, and Burp Suite	4th edition	Packt Publishing
Recommended reading				
Hassan Nihad A.	2018	Open Source Intelligence Methods and Tools : A Practical Guide to Online Intelligence	1st edition	Apress
Rajesh K. V. N.	2024	Ultimate Microsoft Cybersecurity Architect SC-100 Exam Guide	1st edition	Orange Education PVT Ltd

A strategy for evaluating practical assignments and guidelines for using AI (Artificial intelligence) generative models.

In preparing the research project the student must use credible internet sources and scholarly articles and may use AI generative models in accordance with the principles of academic integrity policy (*Copy-Paste* is considered plagiarism - citations must be used, **see below for more details**).
More detailed instructions for the research project and presentation are given to students at the time of topic/case selection.

Examples of the use of AI generative models
The best way to use such tools is:

- When explaining the principles of methods, algorithms and techniques during the learning process,
- for explaining concepts,
- for the development of a structure,
- generating ideas,
- case studies,
- generating summaries (for further work),
- processing large texts (for further work).

All information generated by AI tools **must be verified** and **the work must be referenced to external sources to prove it**, ensuring proper citation (in any case, the Copy-Paste principle is considered plagiarism if no citation is given). It is also important to

understand that AI generative models are not co-authors of the work. More about academic integrity at VU (in particular, see point 19): https://www.vu.lt/site_files/Studies/Study_regulations/Code_of_academic_ethics_VU.pdf.

When should AI generative models <u>not</u> be used in this course?
These tools cannot be used:

- In written work and presentations, for copy-paste submissions without appropriate citation.
- For text embellishment (this does not apply to machine translation tools such as *Deepl*).
- For assessment tests during the semester and exams.

If AI generative models have been used in the preparation of the work?
If AI generative models have been used to generate ideas for the work, it must start with a description of

- The strategy for using AI tools,
- what questions were asked,
- what result was obtained and what percentage of the result was modified and adapted for the work.

The annexes shall contain the queries (e.g. Chat GPT query: "...") and the results (e.g. Chat GPT generated response "...") and the name, version and date of use of the generative model. More on citation: https://apastyle.apa.org/blog/how-to-cite-chatgpt, https://guides.library.uq.edu.au/referencing/chatgpt-and-generative-ai-tools. It must also describe the volume of text generated by the AI tools used in the work. If the text is copied from generative model systems, it must be cited, as must any source. The number of citations and AI-generated text in the thesis cannot exceed 20% (e.g. more https://plagiarismcheck.org/blog/what-is-the-acceptable-percentage-of-plagiarism/).
When using AI generative models, it is important for students to be critical of the answers given, to be ethical, to be accurate, and for each student to be transparent with the rest of the group.

In the case of academic dishonesty: the lecturer informs the administration if he/she notices signs of plagiarism or if he/she discovers that a piece of written work contains blocks of text generated by artificial intelligence tools (i.e. academic dishonesty is suspected). In this case, a process for assessing academic integrity will be initiated.