COURSE UNIT DESCRIPTION

Course unit title	Course unit code
METHODS OF ETHICAL HACKINGS	

Lecturer (s)	Department where course unit is delivered
Lecturer Doc. Dr. Šarūnas Grigaliūnas	Institute of Social Sciences and Applied Informatics Kaunas Faculty 8 Muitines st, LT-44280 Kaunas

Cycle	Level of course unit	Type of the course unit
First	1	Compulsory

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

Prerequisites and corequisites	
Prerequisites:	**Corequisites:**

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

Purpose of the course unit: programme competences to be developed		
To acquaint students with state-of-the-art network hacking techniques and apply them by using only name security screening.		
Learning outcomes of 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, Team project, 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		

	Contact work hours							Individual work hours and tasks	
Course content: breakdown of the topics	**Lectures**	**Consultations**	**Seminars**	**Practiceclasses**	**Laboratory**	**Practice**	**Allcontactwork**	**Individualwork**	**Tasks**
Introduction to Hacking - Ethical Hacking: A Beginner's Guide.	**2**			**2**			**4**	**6**	Analysis of literature, Practical assignments
The Operations Management and Workplace Preparation	**2**			**4**			**6**	**7**	Analysis of literature
The Kill Chain in Cyberspace.	**2**			**2**			**4**	**5**	Practical preparation of the environment
Obtaining the information.	**1**			**2**			**3**	**6**	Analysis of literature, Practical assignments
The scanning overviews. Network scanning.	**1**			**2**			**3**	**6**	Analysis of literature, Practical assignments
The scanning techniques. Network scanning.	**1**			**4**			**5**	**6**	Analysis of literature, Practical assignments
Vulnerability scanning. Network scanning and vulnerability scanning.	**2**			**4**			**6**	**7**	Analysis of literature, Practical assignments
Vulnerability tools.	**1**			**4**			**5**	**7**	Analysis of literature, Practical assignments
Auditing of passwords.	**1**			**2**			**3**	**8**	Analysis of literature, Practical assignments
Shell: Meterpreter.	**1**			**2**			**3**	**6**	Analysis of literature, Practical assignments
Network flows in network behavior.	**1**			**2**			**3**	**7**	Analysis of literature, Practical assignments
OSSTMM and case analysis.	**1**			**2**			**3**	**6**	Analysis of literature
Final examination		**2**				**2**			
TOTAL	**16**	**2**		**32**		**2**	**52**	**78**	

Assessment strategy	**Comparative weight percentage**	**Date of examination**	**Assessment criteria**
Laboratory assignments	60 (4x15)	During semester	Four defenses of laboratory works are planned (sections: 3, 4, 5-6, 11). During the defense of laboratory works, will the tasks during practical classes.

Final examination	40	During Session	Evaluation scale: 10-9: excellent knowledge and skills. 90-100% of correct answers. 8-7: good knowledge and skills, answers may contain some minor errors. Synthesis level. 70-89% of correct answers. 6-5: average knowledge and skills, answers contain numerous errors. Level of analysis. 50-69% of correct answers. 4-3: poor knowledge and skills, below average, answers contain fundamental errors. Knowledge of the level. 20-49% of correct answers. 2-1: knowledge and skills do not conform to minimum requirements. 0-19% of correct answers. Thirty questions are given during the exam, which the examinee must answer in writing (test). The answers to the exam questions are evaluated by 20 theory questions of 1% and ten practice questions of 2% each, for 40%.

Author	Year	Title	Number of periodical publication or publication volume	The place of publication and publisher or online link
Compulsory reading				
1. Peter Kim	2014	The Hacker Playbook 2: Practical Guide To Penetration Testing		CreateSpace Independent Publishing Platform
2. Pat Engebretson	2013	Basics of Hacking & Penetration Testing	2nd Edition	Syngress.
3. Justin Hutchens	2014	Kali Linux Network Scanning Cookbook		PACKT Publishing
Optional reading				
4. Michael E. Whitman, Herbert J. Mattord	2011	Hands-on Informationsecurity Lab Manual	3th edition	Course Technology, Cengage Learning.
5. Stuart McClure, Joel Scambray, George Kurtz	2006	Apsauga nuo hakerių		Smaltijos leidykla.
6. Pete Herzog	2010	The Open Source Security Testing Methodology Manual	3th edition	ISECOM