COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Internet Application Penetration Testing	**ITIAPT**

Lecturer	Department where the course unit is delivered
Coordinator: Lecturer Virgilijus Krinickij	Department of Computational and Data Modeling Faculty of Mathematics and Informatics Vilnius University

Cycle	Type of the course unit
First	Optional

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	4^{th},6^{th} semester	Lithuanian and English

Prerequisites
Common understanding of UNIX operating systems, database management systems, internet technologies.

Number of ECTS credits allocated	Student's workload	Contact hours	Individual work
5	113	48	65

Purpose of the course unit: programme competences to be developed		
Generic competences to be developed • Ability to apply knowledge in practical situations *(BK1)* • Ability for abstract thinking, processing and analysing information *(BK3)* • Ability to resolve problems *(BK4)* ***Subject-specific competences to be developed*** • Ability to do program and IT service testing and debugging *(DK4)* • Ability to evaluate the need of the organization for hardware based on working principles of different computer architectures and various devices *(DK7)* • Ability to ensure information security using management and security mechanisms of operating systems and software *(DK8)*		
Learning outcomes of the course unit	**Teaching and learning methods**	**Assessment methods**
Describe and identify potential risks of cyber-attacks to online applications. Ability to assess possible attack difficulty and attack vector.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.
Vulnerability analysis. Applying best practices for security.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.
Security audit, solutions.	Cooperative lecture, situation analysis, project tasks, consulting.	Written exam, project task assessment.

Course content: breakdown of the topics	**Contact hours**							**Individual work: time and assignments**	
	Lectures	*Consulting during lectures*	Seminars	Tutorials	Laboratory work (LW)	*Consulting during LW*	**Contact hours**	**Individual work**	**Assignments**
1. Introduction to Perimeter Testing of Internet Applications.	2				*4*		**6**	**2**	Preparation of laboratory environment.

2. Security testing phases, malicious code, ethical hacking.	*2*				*4*		**6**	**4**	Working in a laboratory environment, applying general knowledge.
3. Security testing systems, vulnerabilities, attack vectors.	*2*				*4*		**6**	**10**	Laboratory work.
4. Steps for testing the security of online applications.	*2*				*4*		**6**	**10**	Laboratory work.
5. Threat modeling.	*2*				*4*		**6**	**10**	Laboratory work.
6.Vulnerability analysis.	*2*				*4*		**6**	**15**	Laboratory work.
7. Social Engineering.	*2*				*4*		**6**	**6**	Laboratory work.
8. Security audit.	*2*				*4*		**6**	**6**	Laboratory work.
Exam prepara-tion		*2*						**2**	Consulting, material reading
Total:	**16**				***32***		**48**	**65**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Exam written	70%	At the end of the course	Correct answers. Without collecting 15% of 30% from the project work, exam participation is not allowed.
Project work	30%	During the semester	Ability to apply security technologies in different cases.

Author	Publishing year	Title	Issue No or volume	Publishing house or Internet site
Required reading				
Phillip L. Wylie, Kim Crawley	2020	The Pentester BluePrint: Starting a Career as an Ethical Hacker 1st Edition		John Wiley and Sons
Optional reading				
Adam Shostack	2014	Threat Modeling: Designing for Security 1st Edition		John Wiley and Sons
Dafydd Stuttard, Marcus Pinto	2011	The Web Application Hacker's Handbook, 2nd Edition		John Wiley and Sons