COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Website Security Testing (I Part)	**ITWSTFP**

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

Cycle	Type of the course unit
First	Individual

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	Autumn	Lithuanian and English

Prerequisites
General understanding of UNIX operating systems, Programming, and IT basics.

Number of ECTS credits allocated	Student's workload	Contact hours	Individual work
5	99	48	50

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 validate the specification during project implementation (DK3-2)
- 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	Contact hours	Individual work: time and assignments

topics	Lectures	*Consulting during lectures*	Seminars	Tutorials	Laboratory work (LW)	*Consulting during LW*	**Contact hours**	**Individual work**	**Assignments**
1 Introduction, scope.	*2*				*4*		**4**	**2**	Preparation of laboratory environment.
2. Legal boundaries, ethical hacking, and penetration testing workflow.	*2*				*4*		**4**	**3**	Preparing the workflows for ethical hacking.
3. Modern web application structure.	*2*				*4*		**4**	**5**	Websites with Flask, Node or Angular presentation and capabilities.
4. Introduction to web application intelligence, methodologies (OWASP Top 10, „Cyber Kill Chain'').	*2*				*4*		**4**	**7**	Cyber Kill Chain Recon phase on the provided websites.
5. Third-party dependencies and weak architectural signals (APIs, libraries, DBs, technologies).	*2*				*4*		**4**	**7**	Cyber Kill Chain scanning phase on the provided websites.
6. Penetration testing mindset and practical attack planning.	*2*				*4*		**4**	**10**	Cyber Kill Chain attacking phase on the provided websites.
7. XSS, CSRF, other OWASP Top 10 attacks.	*2*				*4*		**4**	**5**	OWASP top 10 related attacks on the provided websites.
8. SQL attacks, other OWASP Top 10 attacks.	*2*				*4*		**4**	**5**	OWASP top 10 related attacks on the provided websites.
Exam preparation								**6**	Consulting, material reading
Total:	**16**				*32*		**48**	**50**	

Assessment strategy	**Weight %**	**Deadline**	**Assessment criteria**

Exam	70%	At the end of the course	The number of correct answers to the questions asked.
Project work	30%	During the semester	Ability to apply security and general IT technologies, methodologies, tools, in different cases. The exam is allowed to be taken if 1.5 out of 3 points are collected in the project part.

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	Nr .1	John Wiley and Sons
Orhan Yildirim	2026	Agentic AI for Offensive Cyber Security	Nr .1	Packt
Andrew Hoffman	2024	Web Application Security 2nd Edition	Nr. 2	O'Reilly Media

DALYKO APRAŠAS

Dalyko pavadinimas	Kodas
Svetainių saugumo testavimas (I dalis)	**ITSSTID**

Dėstytojas	Padalinys
Koordinuojantis: Jaun. Asist. Virgilijus Krinickij	Kompiuterinio ir duomenų modeliavimo katedra Matematikos ir informatikos fakultetas Vilniaus universitetas

Studijų pakopa	Dalyko tipas
Pirmoji	Individualus

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalbos
Auditorinė	Rudens	Lietuvių ir anglų

Reikalavimai studijuojančiajam
Bendro pobūdžio suvokimas apie UNIX operacines sistemos, programavimą ir IT pagrindus.

Dalyko apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	99	48	50

Dalyko tikslas: studijų programos ugdomos kompetencijos

Bendrosios kompetencijos:

- žinias taikyti praktikoje *(BK1)*,
- abstrakčiai mąstyti, analizuoti ir sisteminti informaciją *(BK3)*,
- spręsti problemas *(BK4)*.

Dalykinės kompetencijos:

- testuoti, derinti programas ir IT paslaugas *(DK4),*
- patvirtinti specifikaciją projekto įgyvendinimo metu. *(DK3-2)*
- užtikrinti informacijos saugumą panaudojant operacinių sistemų ir programinės įrangos valdymo bei apsaugos mechanizmus *(DK8)*.

Dalyko studijų siekiniai	Studijų metodai	Vertinimo metodai
Gebėjimas apibūdinti ir nustatyti, galimų kibernetinių atakų internetinėms aplikacijoms rizikas. Gebėjimas įvertinti galimos atakos sunkumą ir atakos vektorių.	Įtraukiamoji paskaita, situacijų analizė, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Gebėjimas nustatyti pažeidžiamumą, atakos vektorių, modeliuoti grėsmes.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Gebėjimas pritaikyti geriausias praktikas saugumui užtikrinti.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Gebėjimas įvertinti esamos kritinės ir nekritinės infrastruktūros komponentus, jau esamus įdiegtus saugumo sprendimus ir įdiegti galimus patobulinimus.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.
Žinos lankstu saugumą, saugumo auditą, sprendimo būdų pritaikymą.	Įtraukiamoji paskaita, situacijų analizė, gerų praktikų studija, projektinė veikla, konsultavimas.	Egzamino testas, projektinių užduočių atlikimas.

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos (P)	*Konsultacijos (P)*	Seminarai	Pratybos	Laboratoriniai darbai	*Konsultacijos (LD,)*	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Įvadas, apimtis.	2				*2*		**4**	**2**	Laboratorinės aplinkos pasiruošimas.

2. Teisinės ribos, etinis įsilaužimas ir įsiskverbimo testavimo darbo eiga.	*2*				*2*		**4**	**3**	Plano paruošimas etiniam įsilaužimui.
3. Šiuolaikinė interneto aplikacijų struktūra.	*2*				*2*		**4**	**5**	Svetainės su „Flask“, „Node“ arba „Angular“ pristatymas su pažeidžiamumais.
4. Įvadas į internetinių aplikacijų žvalgybą, metodikos (OWASP Top 10, „Cyber Kill Chain‘‘).	*2*				*2*		**4**	**7**	„Cyber Kill Chain“ žvalgybos etapas pateiktose svetainėse.
5. Trečiųjų šalių priklausomybės ir silpni architektūriniai signalai (API, bibliotekos, DB, technologijos).	*2*				*2*		**4**	**7**	„Cyber Kill Chain“ skenavimo etapas pateiktose svetainėse.
6. Įsilaužimo testavimo mąstysena ir praktinis atakų planavimas.	*2*				*2*		**4**	**10**	„Cyber Kill Chain“ atakų etapas pateiktose svetainėse.
7. XSS, CSRF, kitos OWASP Top 10 atakos.	*2*				*2*		**4**	**5**	OWASP Top 10 susijusių atakų pateiktose svetainėse realizavimas.
8. SQL atakos, kitos OWASP Top 10 atakos.	*2*				*2*		**4**	**5**	OWASP Top 10 susijusių atakų pateiktose svetainėse realizavimas.
Pasiruošimas egzaminui ir jo laikymas								**6**	
Iš viso	**16**				***32***		**48**	**50**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Projektinis darbas	30%	Pratybų metu	Gebėjimas pritaikyti saugumo ir bendras IT technologijas, metodikas, įrankius, skirtingais atvejais. Egzaminą leidžiama laikyti, jei iš projektinės dalies yra surinkta 1.5 iš 3 balų.
Egzaminas	70%	Semestro pabaigoje	Teisingų atsakymų kiekis į pateiktus klausimus.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr.** **ar leidinio tomas**	**Leidimo vieta ir leidykla** **ar internetinė nuoroda**
Privalomoji literatūra				

Phillip L. Wylie, Kim Crawley	2020	The Pentester BluePrint: Starting a Career as an Ethical Hacker 1st Edition	Nr .1	John Wiley and Sons
Andrew Hoffman	2024	Web Application Security 2nd Edition	Nr. 2	O'Reilly Media
Orhan Yildirim	2026	Agentic AI for Offensive Cyber Security	Nr .1	Packt