DALYKO APRAŠAS

Dalyko pavadinimas	Kodas
Tinklų saugumas	**ITSEQ**

Dėstytojas	Padalinys
Koordinuojantis: prof. dr. Linas Bukauskas kiti: Virgilijus Krinickij.	Kibernetinio saugumo laboratorija Informatikos institutas Matematikos ir informatikos fakultetas Vilniaus universitetas

Studijų pakopa	Dalyko tipas
Pirmoji	Privalomasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalbos
Auditorinė	6 semestras	Lietuvių ir anglų

Reikalavimai studijuojančiajam
Išankstiniai reikalavimai: Studentui reikia turėti bazines kompiuterinio tinklo žinias, duomenų perdavimo metodus, suprasti OSI/TCP/IP modelius, žinoti kompiuterinio tinklo komponentus.

Dalyko apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	125	50	75

Dalyko tikslas: studijų programos ugdomos kompetencijos

Bendrosios kompetencijos:

- žinias taikyti praktikoje *(BK1)*,
- abstrakčiai mąstyti, analizuoti ir sisteminti informaciją *(BK3)*,
- įgyti informacinių ir komunikacijos technologijų naudojimo patirties *(BK5)*.

Dalykinės kompetencijos:

- testuoti ir derinti programas ir IT paslaugas *(DK4)*,
- įvertinti organizacijos poreikį kompiuterinei technikai atsižvelgiant į įvairių tipų kompiuterių architektūros ir atskirų įrenginių veikimo principus *(DK7)*,
- užtikrinti informacijos saugumą panaudojant operacinių sistemų ir programinės įrangos valdymo bei apsaugos mechanizmus *(DK8)*.

Dalyko studijų siekiniai	Studijų metodai	Vertinimo metodai
Taikyti saugaus informacijos perdavimo principus. Kurti kompiuterinio tinklo modelius naudojant įvairius komponentus.	Demonstravimas, atvejų analizė.	Kontrolinis. Egzamino klausimai
Identifikuoti pagrindinės grėsmėmis ir diegti kontrolės priemones grėsmių valdymui/šalinimui. Analizuoti atakų tipus ir veikimo principus.	Laboratoriniai darbai. Užduotys su Kali Linux taikomosiomis programomis.	Praktinis užsiėmimas, namų darbai.
Rinkti informaciją apie atakos objektą; analizuoti pažeidžiamumus; analizuoti bevielio tinklo grėsmes ir atakų metodus; sukurti duomenų srauto stebėsenos modelį diegti kontrolės priemones šnipinėjimo ir adreso klastojimo (sniffing/spoofing) grėsmėms valdyti;	Laboratoriniai darbai. Užduotys su Kali Linux taikomosiomis programomis.	Praktinis užsiėmimas, namų darbai, atsiskaitymas.

paaiškinti slaptažodžių atakų tipus ir veikimo principus; tirti incidentus ir rinkti įrodymus apie įsilaužimą.		
Valdyti technines ir administracines informacijos saugos kontrolės priemones.	Geriausi praktikų/standartų taikymas. Techninių ir administracinių kontrolės priemonėmis palyginimas ir analizė.	Kontrolinis. Egzamino klausimai.
Kurti tinklo architektūrą atsižvelgiant į duomenų kritiškumą ir sistemų funkcionalumą.	Prezentacija. Tinklo architektūros projektavimas ir principai	Namų darbai argumentuojant pasirinktą tinklo modelį.

Temos	**Kontaktinio darbo valandos**							**Savarankiškų studijų laikas ir užduotys**	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Viso kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Saugaus kompiuterinio tinklo architektūra	2						**2**	**2**	Literatūros analizė. Diskusija.
2. Kompiuterių tinklo komponentai. Saugus duomenų perdavimas. Metodai.	2				4		**6**		Literatūros analizė Praktinės užduotys.
3. Tinklo pažeidžiamumai. Atakos.	2				24		**26**	**13**	Praktinės užduotys. Kontroliniai darbai. Namų darbai
4. Tinklo stebėjimas (monitoring)	2				4		**6**		Kontroliniai darbai. Namų darbai
5. Duomenų saugos gairės ir taikymas	2						**2**	**4**	Literatūros analizė. Diskusija. Praktinės užduotys.
6. Aplikacijų sauga. Prieigos kontrolė	2						**2**		
7. Saugus duomenų valdymas. CIA	4						**4**	**2**	
Pasiruošimas egzaminui ir egzamino laikymas		2					**2**	**4**	Egzaminas
Iš viso	**16**	**2**			**32**		**50**	**25**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Namų darbai. Praktinės	20	Semestro	Semestro metu bus siūloma atlikti projektines užduotis

užduotys		metu	asmeniškai ar grupe. Bendra projekto vertė 2 balai Vertinimo schema: 0 - neatliktas arba nekorektiškas darbas arba studentas nesupranta užduoties sprendimo ar negali atlikti keitimų, 0,25 – minimalus atlikimas, ir sunkiai paaiškina ar pakeičia pristatomo projekto programinius sprendinius 0,5 – darbas atliktas nepilnai ir dalinai geba paaiškinti ar dalinai pakeičia, 1 - atlikta puikiai studentas geba paaiškinti sprendimą ir geba keisti veikimo parametrus.
Egzaminas	80	Semestro pabaiga	Egzamino vertė 8 balai: Egzaminas yra iš teorijos ir praktinių užsiėmimų metu įgytų žinių ir gebėjimų

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privalomoji literatūra				
Shon Harris	2012	CISSP All-in-One Exam Guide. 6th edition		McGraw-Hill
James Broad	2013	Penetration Testing with Kali		Elsevier
Papildoma literatūra				
Charlie Kaufman, Radia Perlman, Mike Speciner	2002	Network Security: Private Communication in a Public World. 2nd edition		Prentice Hall
		PCI-DSS V2 security standard	https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0	
		ISO/IEC 27002 security standard. 27002:2009	http://www.lsd.lt/standards/catalog.php?ics=0&pid=634586	

COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Network Security	**ITSEQ**

Lecturer	Department where the course unit is delivered
Coordinator: prof. dr. Linas Bukauskas other: Virgilijus Krinickij	Cybersecurity laboratory Institute of Computer Science Faculty of Mathematics and Informatics Vilnius University

Cycle	Type of the course unit
First	Compulsory

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

Prerequisites
Student should have basic knowledge of networking, data transfer methods, understand OSI/TCPIP models, understand networking components.

Number of ECTS credits allocated	Student's workload	Contact hours	Individual work
5	125	50	75

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 use information and communications technologies *(BK5)*

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
Ability to apply secure data transfer methods. Ability to design network models using various units.	Presentation. Case study/analysis.	Evaluation test, exam.
Ability to identify top threats and implement appropriate controls. Ability to analyse attack types and exploitation principles.	Practical exercises using KALI Linux distribution components	Homework and classwork.
Ability to do: object enumeration; vulnerability analysis; analysis of wireless network treats and attack methods. Ability to implement: monitoring model, controls/solution to prevent sniffing and spoofing.	Practical exercises using KALI Linux distribution components	Homework and classwork Evaluation test.

Ability to explain password attack types and principles. Ability to undergo incident and investigation (evidence gathering).		
Ability to manage technical and administrative security controls.	Best practices and security standards analysis and mapping. Compliance management.	Evaluation test. Exam
Ability to make network design and architecture models based on data sensitivity and system functionality.	Presentation. Network architecture and design principals	Homework

Course content: breakdown of the topics	**Individual work: time and assignments**							
	Lectures	Tutorials	Seminars	Laboratory work	Internship/work placement	**Contact hours**	**Individual work**	**Assignments**
1. Secure network architecture	2					**2**	**2**	Literature analysis. Discussion
2. Networking components. Secure data transfer methods.	2			4		**6**		Literature analysis. Classwork
3. Network vulnerabilities. Attack types.	2			24		**26**	**13**	Classwork, tests, homework.
4. Network monitoring	2			4		**6**		Test, homework.
5. Information security framework and governance	2					**2**	**4**	Literature analysis. Discussion. Classwork and homework.
6. Application security. Logical access management.	2					**2**		
7. Secure data management. [Confidentiality, Integrity Availability]	4					**4**	**2**	
Exam preparations		2				**2**	**4**	Exam
Total	**16**	**2**		**32**		**50**	**25**	

Assessment strategy	**Weight %**	**Deadline**	**Assessment criteria**
Homework and classwork	20	During semester	During the semester, students will be offered project tasks to complete individually or in groups. Total project value: 2

			points Assessment scheme: 0 – work not completed or incorrect, or the student does not understand the task or is unable to make changes 0.25 - minimal completion, and has difficulty explaining or changing the program solutions of the presented project 0.5 - work is incomplete and the student is partially able to explain or partially change it, 1 - completed excellently, the student is able to explain the solution and is able to change the operating parameters. Translated with DeepL.com (free version)
Exam	80	End of semester	Exam evaluation - 8 points. Exam consists of:

Author	**Publishing year**	**Title**	**Issue No or volume**	**Publishing house or Internet site**
Required reading				
Shon Harris	2012	CISSP All-in-One Exam Guide. 6th edition		McGraw-Hill
James Broad	2013	Penetration Testing with Kali		Elsevier
Optional reading				
Charlie Kaufman, Radia Perlman, Mike Speciner	2002	Network Security: Private Communication in a Public World. 2nd edition		Prentice Hall
		PCI-DSS V2 security standard	https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0	
		ISO/IEC 27002 security standard. 27002:2009	http://www.lsd.lt/standards/catalog.php?ics=0&pid=634586	