COURSE SYLLABUS AND COURSE REQUIREMENTS
ACADEMIC YEAR 2023/2024 SEMESTER 2

Course title	*Information Security 1.*
Course Code	IVB165ANMI
Hours/Week: le/pr/lab	2/0/3
Credits	5
Degree Programme	Computer Science Engineering
Study Mode	*full time course*
Requirements	Exam
Teaching Period	spring
Prerequisites	IP Based Systems and Applications
Department(s)	System and Software Technology
Course Director	Gábor Gyurák
Teaching Staff	*Gábor Gyurák*

COURSE DESCRIPTION

This course is intended to help students gain fundamental and comprehensive understanding of information security. We will focus on an overview of major information security issues, technologies, and approaches. Students who successfully complete this course will have a concept and knowledge of security properties, concerns, policies, models, cryptography, PKI, firewalls, security evaluation, and real life security cases. Students will also have hands on experience in selected information security technologies through lab sessions.

SYLLABUS

1. GOALS AND OBJECTIVES

Course goals:

- To provide an understanding of principal concepts, major issues, technologies, and basic approaches in information security.
- To provide concept level hands on experience in specific topic area.
- To provide the ability to examine and analyse real life security cases.

Learning Objectives:
Students who successfully complete this course will have a comprehensive overview of information security as well as more in depth understanding of a number of focus areas that they select throughout the course. Furthermore, students will have hands on experiences in information security.

2. COURSE CONTENT

Neptun: Instruction/Subjects/Subject Details/Syllabus/Subject content

	TOPICS
LECTURE AND PRACTICE	*Harden servers and clients.* *Recognize common attack patterns.* *Evaluate vulnerability of an information system and establish a plan for risk management.* *Demonstrate how to detect and reduce threats in Web security.* *Evaluate the authentication and encryption needs of an information system.* *Explain the Public Key Infrastructure process.* *Demonstrate how to secure a wireless network.* *Evaluate a company's security policies and procedures.*

DETAILED SYLLABUS AND COURSE SCHEDULE

LECTURE

week	**Topic**	**Compulsory reading; page number (from … to …)**	**Required tasks (assignments, tests, etc.)**	**Completion date, due date**
1.	Course introduction, orientation	-	-	-
2.	Cybersecurity concepts	[1] chapter 1	-	-
3.	Cybersecurity cube, CIA model	[1] chapter 2	-	-
4.	Threats, Vulnerabilities, Attacks	[1] chapter 3	-	-
5.	Protecting secrets	[1] chapter 4	-	-
6.	Ensuring Integrity	[1] chapter 5	-	-
7.	The five nines concept	[1] chapter 6	-	-
8.	Securing a small network	[1] chapter 7	-	-
9.	Symmetric cryptography	[1] chapter 8	-	-
10.	Asymmetric cryptography	[1] chapter 9	-	-
11.	PKI, digital signatures	[1] chapter 10	-	-
12.	TEST	-	TEST	-
13.	Break	-	-	
14.	RETAKE TEST	-	RETAKE TEST	-

PRACTICE, LABORATORY PRACTICE

week	**Topic**	**Compulsory reading; page number (from … to …)**	**Required tasks (assignments, tests, etc.)**	**Completion date, due date**
1.	CMS registration	-	-	-
2.	Reconnaissance, protocol analysis	[2] chapter 1	-	-
3.	Scanning	[2] chapter 2	-	-
4.	Sniffing	[2] chapter 3	-	-
5.	Exploitation 1	[2] chapter 4	-	-
6.	Exploitation 2	[2] chapter 5	-	-
7.	WEB security	[2] chapter 6	-	-
8.	VLANS 1	[2] chapter 7	-	-
9.	DoD attacks	[2] chapter 8	-	-
10.	VLANS 2	[2] chapter 9	-	-
11.	Redundant systems	[2] chapter 10	-	-
12.	TEST	-	TEST	
13.	Break	-	-	-
14.	RETAKE TEST	-	RETAKE TEST	-

3. ASSESSMENT AND EVALUATION

ATTENDANCE

In accordance with the Code of Studies and Examinations of the University of Pécs, Article 45 (2) and Annex 9. (Article 3) a student may be refused a grade or qualification in the given full-time course if the number of class absences exceeds 30% of the contact hours stipulated in the course description.

Method for monitoring attendance *(e.g.: attendance sheet / online test/ register, etc.)*

attendance sheet

ASSESSMENT

Course-unit with final examination

Mid-term assessments, performance evaluation and their weighting as a pre-requisite for taking the final exam

Type	Assessment	*Weighting as a proportion of the pre-requisite for taking the exam*
TEST	*max. 100%*	*100%*

Requirements for the end-of-semester signature

TEST result is greater than or equals to 40%

Re-takes for the end-of-semester signature (PTE TVSz 50§(2))

The specific regulations for grade betterment and re-take must be read and applied according to the general Code of Studies and Examinations. E.g.: all the tests and the records to be submitted can be repeated/improved each at least once every semester, and the tests and home assignments can be repeated/improved at least once in the first two weeks of the examination period.

Reatek test is scheduled to the 15th week.

Type of examination *(written, oral): written*

The exam is successful if the result is minimum 40 %

Calculation of the grade *(TVSz 47§ (3))*

The mid-term performance accounts for ***50*** %, the performance at the exam accounts for ***50*** % in the calculation of the final grade.

Calculation of the final grade based on aggregate performance in percentage.

Course grade	Performance in %
excellent (5)	85 % …
good (4)	70 % ... 85 %
satisfactory (3)	55 % ... 70 %
pass (2)	40 % ... 55 %
fail (1)	below 40 %

The lower limit given at each grade belongs to that grade.

4. SPECIFIED LITERATURE

In order of relevance. (In Neptun ES: Instruction/Subject/Subject details/Syllabus/Literature)

COMPULSORY READING AND AVAILABILITY

[1.] William Stallings, Lawrie Brown, Computer Security Principles and Practice, 2012.
[2.] Chuck Easttom, Computer Security Fundamentals, 2006.
[3.] Randy Weaver, Dawn Weaver, Tactical Perimeter Defense: Becoming a Security Network Specialist, 2008

RECOMMENDED LITERATURE AND AVAILABILITY

[1.] Mark Merkow, Jim Breithaupt, Information Security Principles and Practices, 2006.