General Information:

Name of Course: **INFORMATION SECURITY 1.**

Course Code: IVB165ANMI
Semester: **5**th
Number of Credits: 5
Allotment of Hours per Week: 2 Lectures, 3 practical classes /Week
Evaluation: Exam (with grade)
Prerequisites: **IP Based Systems and Applications**

Instructor: **Gábor GYURÁK, assistant lecturer**
Office: H-7624 Pécs, Boszorkány u. 2. Office N° B-144
Office hours: Friday 12:00-13:00
E-mail: gyurak@mik.pte.hu

Introduction, General 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.

Course aims:

- 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. At the end of the semester, the students will be able to

- 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.

Methodology:

- **Lectures**: discussion and lectures on IT security theory.
- **Practical class**: will give an introduction securely of planning, building, programming and operating IT systems.

Schedule:

Week	Lecture	Practical class
Week 1	Course introduction, orientation	CMS registration, laboratory guide
Week 2	Computer security concepts	Reconnaissance, protocol analysis
Week 3	Threats, attacks and assets	Scanning
Week 4	AAA model	Sniffing
Week 5	AI in security	Exploitation 1
Week 6	IT security standards	Exploitation 2
Week 7	***T1 test***	
Week 8	Symmetric cryptography	WEB security
Week 9	*Autumn break – no classes*	
Week 10	Risk management	Management plane security
Week 11	Asymmetric cryptography	Firewalls
Week 12	Digital signature	PKI
Week 13	Intrusion Detection	IDS systems
Week 14	Student presentations part1	***T2 test***
Week 15	Student presentations part2	***RT test***

Attendance:
Attending is required all classes, and will impact the grade (max. 10%). Unexcused absences will adversely affect the grade, and in case of absence from more than 30% of the total number of lesson will be grounds for failing the class. To be in class at the beginning time and stay until the scheduled end of the lesson is required, tardiness of more than 20 minutes will be counted as an absence. In the case of an illness or family emergency, the student must present a valid excuse, such as a doctor's note.

Evaluation + Grading:
The course grade is determined as a combination of study-period performance (midterm tests and homework) and the exam (in some cases exam is replaceable with pre-exam).
All exams and tests are closed-book and closed-notes. Any students who do not take the examination at the scheduled time will receive a zero score.

The study period performance is successful and the student get a signature if

- the average of T1 and T2 is greater than or equals to 50% → (T1+T2)/2 >= 50%
    - if the average is less than 50% the student can retake the tests with <u>one</u> complex retake-test (RT) scheduled to the last week.
        - in this case student get a signature only if (((T1+T2)/2)+RT)/2>=50%
- and the student solved and presented the homework

This course ends with an exam (E):

- The exam can be taken only after a successful study period, only if the student got the signature
- The course grade is calculated by the average of the study period performance and the result of the exam.

<u>Course performance evaluation:</u>

- Without retake-test: Performance=((T1+T2)/2+E)/2
- With retake-test: Performance=(((((T1+T2)/2)+RT)/2)+E)/2

Grade:	5	4	3	2	1
Evaluation in percent:	81%-100%	71%-80%	61%-70%	51%-60%	0-50%

PTE Grading Policy:
Information on PTE's grading policy can be found at the following location:
www.pte.hu

Students with Special Needs:

Students with a disability and needs to request special accommodations, please, notify the Deans Office. Proper documentation of disability will be required. All attempts to provide an equal learning environment for all will be made.

Readings and Reference Materials:
Required:

1. Presentation slides (Moodle CMS)
2. William Stallings, Lawrie Brown, Computer Security Principles and Practice, 2012, ISBN-13: 978-0-13-277506-9

More:

1. Chuck Easttom, Computer Security Fundamentals, 2006, ISBN: 0-13-171129-6
2. Randy Weaver, Dawn Weaver, Tactical Perimeter Defense: Becoming a Security Network Specialist, 2008, ISBN-13: 978-1-4283-5630-6
3. Mark Merkow, Jim Breithaupt, Information Security Principles and Practices, 2006, ISBN: 0-13-154729-1