COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security in computer networks

Course

Field of study
Electronics and telecommunications
Area of study (specialization)
Computer networks and Internet technologies
Level of study
Second-cycle studies
Form of study
full-time

Year/Semester
1/2
Profile of study
general academic
Course offered in
Polish
Requirements
elective

Number of hours

Lecture
30
Laboratory classes
15
Other (e.g. online)

Tutorials
15
Projects/seminars

Number of credit points

4

Lecturers

Responsible for the course/lecturer:
dr inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Responsible for the course/lecturer:

Prerequisites

Student knows the most important standards, architectures, protocols and devices of computer networks. He should also understand the need to expand his competences and have the ability to obtain information from specified sources.

Course objective

Presentation the theoretical and practical issues related to building secure computer networks and penetration testing as well as the conscious and safe use of Internet resources.

Course-related learning outcomes

Knowledge

The student has knowledge in the field of computer network security including:

1. principles of operation of solutions ensuring network security (firewalls, IPS / IDS),

2. construction and operation of the VPN network,

3. cryptographic mechanisms used in modern networks,

4. penetration tests

Skills

1. Can configure network devices and software in a way that ensures secure data transfer.

2. Is able to use cryptographic mechanisms for secure data transmission.

3. Is able to plan and carry out simple penetration tests of computer networks.

4. Is able to consciously use Internet resources.

Social competences

1. Is aware of the changes that occur with the evolution of computer networks. Knows the limitations of his own knowledge and understands the need for continuous updating. Is open to the possibility of continuous training.

2. Has professional approach to solving problems related to network security.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture:

Knowledge is verified by an test, which has a written or oral form depending on the size of the group. The test consists of 30 test questions, where 4 answers are proposed, but only one answer is correct. Passing threshold is 50%. Final issues on the basis of which questions are prepared will be sent to students by e-mail using the university e-mail system. In the case of the oral exam, each student answers three questions from the set of 40 (they are known to students). Questions are given by the person conducting the exam. The correctness of the answer and the degree of understanding of the problem by the student are assessed.

Laboratory classes:

Knowledge and skills are verified by checking the correctness of the exercise, e.g. by checking the correct configuration of network devices and asking questions about the exercise. Lack of passing the exercise results in the need to repeat it within the time limit indicated by the teacher.

Tutorials:

Tutorials are evaluated based on a test (written or oral depending on the size of the group). The test consists of four open questions scored depending on their difficulty. Passing threshold is 50%. The issues on the basis of which the questions are developed correspond to the content presented during the exercises.

Programme content

Lecture:

1. Analysis of threats in the Internet

2. Hardware and software network firewalls

3. Security of network devices

4. Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS)

5. Introduction to cryptography

6. Network protocols for safe data transfer

7. VPN (Virtual Private Networks)

8. Penetration tests in computer systems.

Tutorials:

1. Modern Network Security Threats.

2.Analysis of cryptographic mechanisms ensuring safe data transmission.

3. Analysis of network protocols ensuring safe data transmission.

Laboratory classes:

1. Configure hardware firewalls.

2. Configuration of network devices providing secure remote access.

3. Configuration of the hardware intrusion detection system (IDS).

4. Construction of the VPN network.

5. Conduct simple computer network security tests using Kali Linux.

Teaching methods

Lecture: multimedia presentation supplemented with examples and additional explanations on the board. Lectures are conducted in accordance with the principles of traditional lecture, in justified cases taking the form of a conversational lecture.

Laboratory exercises: multimedia presentation, presentation illustrated with examples given on a blackboard, and performance of tasks given by the teacher - practical exercises.

Tutorials: multimedia presentation, presentation illustrated with examples given on a blackboard (cryptografic algorithems, network protocols)

Bibliography

Basic

1. Serafin M., Sieci VPN : zdalna praca i bezpieczeństwo danych, Helion 2008.

2. Kim P., Podręcznik pentestera : bezpieczeństwo systemów informatycznych, Helion 2015.

3. Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii, Helion 2012.

4. Amato V., Akademia sieci Cisco : drugi rok nauki, Mikon 2001

5. Wnag J., Computer network security : theory and practice, Higher Education Press 2009.

6. Tanenbaum A. S., Wetherall D. J., Computer networks, Pearson Longman 2014 .

Additional

1. www.cisco.com

2. Erickson J., Hacking, Sztuka penetracji, Helion 2004

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,0
Classes requiring direct contact with the teacher	70	3,0
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) [1]	30	1,0

[1] delete or add other activities as appropriate