COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of network devices [S2Teleinf2-ZTM>BU]

Course

Field of study
Teleinformatics

Year/Semester
1/2

Area of study (specialization)
Advanced multimedia techniques

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
14

Laboratory classes
24

Other
14

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr hab. inż. Piotr Zwierzykowski prof. PP
piotr.zwierzykowski@put.poznan.pl

Lecturers

Prerequisites

A student starting this course should have knowledge of computer network structure and operation. In particular, they should be familiar with basic protocols that facilitate communication in networks (ARP, IPv4/IPv6, RIP, DHCP). They should also have a basic understanding of probability theory and probabilistics. Additionally, the student should have basic skills in operating Linux operating systems.

Course objective

The aim of the course is to familiarize students with issues related to the security of network devices. The course covers topics related to IoT devices, industrial devices, as well as operator-class and access- class network devices.

Course-related learning outcomes

Knowledge:
Has a expanded and in-depth knowledge of the security of devices included in corporate and industrial ICT networks. (K2_W02)
Knows and understands algorithms used in teleinformatics systems within the specialization area (K2_W05)

Skills:
He/she is able to acquire information from literature, databases, and other sources; integrate the obtained information; interpret and critically evaluate it; draw conclusions; and formulate and thoroughly justify opinions (K2_U01)
Can plan and conduct research experiments, including testing, simulation, measurement of characteristics, parameter extraction, analysis and synthesis of secure ICT systems (K2_U07)

Social competences:
Is ready to fulfill professional roles responsibly, taking into account changing social needs, including developing professional expertise, upholding professional ethics, and adhering to and promoting ethical principles and ensuring compliance with these principles (K2_K06)

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired during the lecture is assessed through a written or oral exam. In the written form, students must answer 6 questions (multiple-choice and open-ended) with different point values. There are three point groups (1, 2, and 3 points). For the oral exam, each student randomly selects two questions from each point group. In the oral form, for each selected question, the student may receive an additional question related to the chosen one. The grade for each question (including the response to both the selected question and the additional question) takes into account the scope of the answer and the depth of understanding of the topic. A total of 60 questions are prepared for each exam. The condition for passing the exam is to receive a minimum of 50% of the possible points.
The grading criteria for the exam are as follows:
Points Earned Grade
<= 6 points 2.0
7-8 points 3.0
9 points 3.5
10 points 4.0
11 points 4.5
12 points 5.0
The skills acquired during the laboratory sessions are assessed based on tasks performed during the classes. Each task is given a grade, and the final grade is the average of all the grades, with the requirement that all tasks receive a passing grade.

Programme content

Presentation and discussion of areas related to ensuring the security of network devices in computer networks.

Course topics

1. Presentation and discussion of areas related to ensuring the security of network devices.
2. Securing routers and switches in corporate IP networks.
3. Secure remote access to network devices (VPN, AAA).
4. Devices providing secure access to network and endpoint devices (firewalls).
5. Supply chain security.
6. Security of IoT devices.
7. Attacks utilizing reconnaissance and methods of protecting against them.
8. Analysis of the functional security of network solutions.

Teaching methods

Lectures: Depending on the topic being discussed and students' interests, the lecture is conducted in one of three formats: traditional lecture (multimedia presentation supplemented with examples written on the board), problem-based lecture (discussion with the audience on solving a specific problem), or conversational lecture (engaging the audience in discussion, directing the lecture based on the answers provided, etc.).
Laboratory exercises: The exercises are conducted in laboratories of Network Academy of Huawei or Cisco. During the sessions, students perform tasks presented by the instructor, which involve properly

connecting devices (switches, routers, and computers) and configuring network devices according to the requirements of each exercise.

Bibliography

Basic:
1. Marek Serafin:Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone, Helion, 2013
2. Marvin Rausand, Reliability of Safety-Critical Systems: Theory and Applications, John Wiley & Sons, 2014

Additional:
1. Omar Santos: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, 2020

Breakdown of average student's workload

	Hours	ECTS
Total workload	78	3,00
Classes requiring direct contact with the teacher	38	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	40	1,50