COURSE DESCRIPTION CARD - SYLLABUS

Course name
Network Security [S2Inf1E-CYB>NET]

Course

Field of study
Computing

Year/Semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
45

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

5,00

Coordinators

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

A student starting this course should have a basic knowledge of ICT security. He should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of the team.

Course objective

Providing students with detailed theoretical knowledge in the field of network security; providing students with the knowledge and skills necessary to design and support network security; familiarizing students with industrial standards for implementing network security solutions and creating opportunities to acquire the skills required for further career development (preparation for certification exams).

Course-related learning outcomes

Knowledge:
has advanced detailed knowledge of selected issues in the field of network security threats and cloud services, methods and tools used to prevent attacks, network security testing techniques.

has knowledge of development trends and the most important new achievements in the field of network device security and secure data transmission techniques; has knowledge of the current security threats to network systems.
knows advanced methods, techniques and tools used in solving complex engineering tasks in the field of network security and ict systems.

Skills:
is able to obtain from various sources information on threats to ict security and techniques for their effective detection and prevention of their use in network systems. obtained information (in polish and english) can integrate and subject to critical evaluation.
can use experimental methods to formulate and solve engineering tasks and simple research problems in the field of ict network security.
can make a critical analysis of the existing technical solutions in the area of security of network solutions and propose their improvements.
can assess the usefulness and the possibility of using new hardware and software solutions for solving engineering tasks consisting in building secure data transmission systems.
can design a system ensuring the security of transmitted data.
can work in a team in the formulation and solving of engineering tasks related to the design and implementation of network systems responsible for the security of transmitted data.
can define the directions of further learning necessary for effective work in the area of network security.

Social competences:
understands that in the field of ict security, knowledge and skills very quickly become obsolete.
understands the importance of using the latest knowledge in the field of ict security in solving research and practical problems. is aware of the need for a professional approach to solved ict security problems and taking responsibility for the projects he proposes.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Knowledge acquired as part of the lecture is verified by a written exam.
Test issues, on the basis of which questions are prepared, are sent to students by e-mail using the university e-mail system.
The written exam consists of from 3 to 5 questions for which a descriptive answer is expected. Each answer to a question is rated on a scale of 0 to 5 points. Each question is scored equally. Passing threshold: 50% of points.
In the case of the oral test, students draw questions from a set of 30 questions. In the case of a written test, questions are selected by the teacher.
Skills acquired as part of the laboratory are verified on an ongoing basis. At the end of each laboratory class, the correctness of configuration of network devices is assessed on a scale of 2 to 5. The final grade is the average of grades obtained from individual laboratory classes.

Programme content

Network security, including device access security, security related to the transmission of network traffic.

Course topics

1. The following topics will be discussed as part of the lecture:
- Network threats and attacks, current state of network security solutions.
- Mitigating threats: security policies, tools, services; securing device access; administrative roles.
- Inroduction to software-defined networking and network programmability.
- Authentication, authorization, accounting and identity management.
- Network Visibility (e.g., NetFlow, IPFIX, etc.).
- Securing Layer 2 (VLANs; threats; IEEE 802.1AE/MACsec+).
- Securing management plane, control plane and data plane of network devices.
- Firewall technologies (review of ACLs; role of firewalls in network design; zone-based policy firewalls).
- Securing networks with ASA.

- Intrusion Detection Systems and Intrusion Prevention Systems (various vendors" implementations; IPS operation and configuration).
- Virtual Private Networks (topologies; protocols; implementations: IPSec, DMVPN, FlexVPN, GETVPN, Client-based remote access VPN, Clientless remote VPN).
- Securing the Cloud.
- Network Security Testing.
2. Laboratory topics:
In line with the content of lectures.

Teaching methods

Informative lecture: multimedia presentation, illustrated with examples on the board.
Laboratory exercises: practical exercises in groups using network devices.

Bibliography

Basic
1. Joseph Migga Kizza: Guide to Computer Network Security; Springer International Publishing, 2020, 10.1007/978-3-030-38141-7.
2. Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021
Additional
1. Khondoker, Rahamatullah (Ed.): SDN and NFV Security - Security Analysis of Software-Defined Networking and Network Function Virtualization; Springer International Publishing 2018.
2. Aaron Woland, Vivek Santuka, Mason Harris, Jamie Sanbower: Integrated Security Technologies and Solutions - Volume I: Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security, May 14, 2018, Cisco Press.
3. Elaine Barker, Quynh Dang, Sheila Frankel, Karen Scarfone, Paul Wouters: Guide to IPsec VPNs (NIST Special Publication 800-77); National Institute of Standards and Technology; 2020; This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-77r1
4. J. Michael Stewart: Network Security, Firewalls And VPNs; Jones & Bartlett Learning Information Systems Security & Ass, 2nd Edition, 2013.
5. Gerardus Blokdyk: IPsec VPN A Complete Guide; 5STARCooks; 2019.

Breakdown of average student's workload

	Hours	ECTS
Total workload	125	5,00
Classes requiring direct contact with the teacher	60	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	65	2,50