COURSE DESCRIPTION CARD - SYLLABUS

Course name
Introduction to Cybersecurity [S2Teleinf2>WdC]

Course

Field of study
Teleinformatics

Year/Semester
1/1

Area of study (specialization)
–

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
24

Laboratory classes
30

Other
24

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

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 basic knowledge of computer networks, cryptographic algorithms, Windows and Linux operating systems. 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 knowledge in the field of broadly understood ICT security as well as methods and tools used to estimate and control the risk of breach of confidentiality, integrity and data availability. To acquaint students with advanced methods, techniques and tools used in solving complex engineering tasks in the area of designing and maintaining network systems responsible for the security of transmitted data. The course covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an Cybersecurity Analyst working in a Security Operations Center (SOC). As part of the course, cybersecurity domains will be discussed as basic elements for managing the cybersecurity of an organization. Presentation of the principles of operation of the Computer Emergency Response Teams, Security Operations Center. Getting to know the assumptions of Security Information and Event Management. As part of the exercises, the student will develop his own SOC concept taking into account real conditions.

Course-related learning outcomes

Knowledge:
Has ordered and theoretically founded general knowledge related to key issues in the field of ICT security [K2_W05].
Has advanced detailed knowledge of selected issues in the field of broadly understood ICT security as well as methods and tools used to estimate and control the risk of breach of confidentiality, integrity and data availability [K2_W06].
Has knowledge of development trends and the most important new achievements of IT and telecommunications in the design and maintenance of network systems responsible for the security of transmitted data [K2_W08].
Has advanced and detailed knowledge of the processes of the systems used to estimate and control the risk of breach of confidentiality, integrity and data availability [K2_W07].
Has knowledge of the ethical principles related to the activities necessary to ensure the security of ICT systems.

Skills:
Can obtain information on ICT security threats and techniques for their estimation and control. Obtained information (in Polish and English) can integrate and subject to critical evaluation [K2_U01].
Can use experimental methods to formulate and solve engineering tasks and simple research problems in the area of ICT security [K2_U03].
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 [K2_U10].
Is able to cooperate in a team responsible for ensuring the security of ICT systems [K2_U02].
Is able to define the directions of further learning in order to meet the challenges posed by people responsible for the security of ICT systems [K2_U11].

Social competences:
Student understands that in the field of ICT security, knowledge and skills very quickly become obsolete [K2_K01]. 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 solving ICT security problems and taking responsibility for the projects he proposes [K2_K06].

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Knowledge acquired as part of the lecture is verified by a written test.
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 test 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

- Fundamentals of Cybersecurity.
- Types of Attacks and Vulnerabilities.
- Fundamentals of Cloud Computing and Cloud Security.
- Fundamentals of IoT Security.
- Fundamentals of Access Contro.
- Review of PKI, Root and Identity Certificates, IPSec, Virtual Private Networks.
- Fundamentals of Security Operations Management.
-Fundamentals of Intrusion Analysis.
- Introduction to Digital Forensic.
- Telemetry and Analysis of Network and End Devices.
- Tasks of Security Operations Centers (SOCs).
- Cybersecurity Models and Threat Hunting.
- Fundamentals of Security and Ethics.

Course topics

1. The following topics will be discussed as part of the lecture:
- Review of TCP/IP protocols.
- Fundamentals of Cybersecurity (NIST; Threats, Vulnerabilities, Exploits; IDS, IPS).
- Types of Attacks and Vulnerabilities.
- Fundamentals of Cloud Computing and Cloud Security (Cloud Models; DevOps, CI/CD; Cloud Security Threats).
- Fundamentals of IoT Security.
- Fundamentals of Access Control (AAA, Processes, Responsibilites, Mechanisms; Identity and Acccess Control Implementations).
- Review of PKI, Root and Identity Certificates, IPSec, Virtual Private Networks.
- Fundamentals of Security Operations Management (Identity and Access Management; Events and Log Management; Assests and Change Managment; Vulnerability Management; CSIRT, SOC, SIEM, SOAR).
- Telemetry and Analysis of Network and End Devices (Logs, Packet Capturing, Network Profiling; Host Profiling.
- Tasks of Security Operations Centers (SOCs).
- Cybersecurity Models and Threat Hunting (Threat modelling, e.g., STRIDE, PASTA, CVSS, Attack treas, etc.;).
- Fundamentals of Security and Ethics.
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. Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021
2. Joseph Migga Kizza: Guide to Computer Network Security; Springer International Publishing, 2020, 10.1007/978-3-030-38141-7

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	104	4,00
Classes requiring direct contact with the teacher	54	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	50	2,00