COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cybersecurity [S1EiT1E>CYBERB]

Course

Field of study
Electronics and Telecommunications

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

Lecture
30

Laboratory classes
15

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

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

Lecturers

Prerequisites

A student joining this course should have basic knowledge of TCP / IP stack protocols. He/she should understand the communication process between network devices and know the basics of operating systems.

Course objective

The aim of the module is to familiarize students with techniques in a “sandboxed” virtual machine environment that allows them to create, implement, monitor, and detect various types of cyber attacks. The module allows the students to study the techniques that threat actors use to circumvent data, privacy, and computer and network security.

Course-related learning outcomes

Knowledge:
1. A student has a systematic knowledge of key technologies of computer and network security.
2. A student has a basic, systematic knowledge of structure, operation and standards related to computer and network security.
3. A student knows the virtual machine environment that allows to create, implement, monitor, and

detect various types of cyber attacks.

Skills:
1. A student is able to select the proper technologies for securing computers and networks.
2. A student has the necessary skills needed to thwart the known and future cyber attacks.
3. A student is able to apply proper mechanisms to detect unauthorized access to data, computer, and network systems.

Social competences:
1. A student knows the limits of his/her own knowledge and skills, understands the need for further training in the field of cybersecurity.
2. A student understands that knowledge and skills in the field of cybersecurity are becoming obsolete very quickly.
3. A student is aware of the need for a professional approach to design solutions based on cybersecurity approach. He/she can effectively participate in team projects.

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 an oral and / or 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 and / or oral 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

- Cybersecurity and the Security Operation Center;
- Principles of network securty;
- Security of Windows operating system;
- Security of Linux operating system;
- Security of network protocols and services;
- Security of network infrastructure;
- Network attacks;
- Methods for protecting a network;
- Cryptography and the public key infrastructure;
- Endpoint security and analysis;
- Security monitoring.

Course topics

1. The following topics will be discussed as part of the lecture:
- Cybersecurity and the Security Operation Center;
- Principles of network securty;
- Security of Windows operating system;
- Security of Linux operating system;
- Security of network protocols and services;
- Security of network infrastructure;
- Network attacks;
- Methods for protecting a network;
- Cryptography and the public key infrastructure;
- Endpoint security and analysis;
- Security monitoring.
2. The following lab exercises will be carried out as part of the laboratory classes:
- Installing the CyberOps Workstation Virtual Machine;

- Monitor and Manage System Resources in Windows;
- Navigating the Linux Filesystem and Permission Settings;
- Using Wireshark to observe network traffic;
- Anatomy of Malware;
- Encrypting and Decrypting Data Using a Hacker Tool;
- Interpret HTTP and DNS Data to Isolate Threat Actor.

Teaching methods

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

Bibliography

Basic
1. William Stallings, Cryptography and network security : principles and practice ; Pearson Education. 2014.
2. William Stallings, Network security essentials: applications and standards, Pearson Education, 2011.
Additional
1. CCNA Cybersecurity Operations Companion Guide, Jun 15, 2018 by Cisco Press.
2. Raef Meeuwisse, Cybersecurity for Beginners, Lulu Publishing Services (May 14, 2015).
3. Lester Evans, Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners, Independently published (January 23, 2019).
4. Curriculum available on the cisco.netacad.net platform as part of the Cisco Network Academy run at the Institute of Communication and Computer Networks.

Breakdown of average student's workload

	Hours	ECTS
Total workload	90	3,00
Classes requiring direct contact with the teacher	55	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	35	1,00