Co-funded by the
Erasmus+ Programme
of the European Union

EUROPEAN UNIVERSITY FOR CUSTOMISED EDUCATION

STUDY GUIDE

CYBERSECURITY

Organised by

Poznan University of Technology (PUT)

1. IDENTIFYING DATA.	
· Course Name.	*Cybersecurity*
· Coordinating University.	*Poznan University of Technology*
· Partner Universities Involved.	*Not applicable*
· Course Field(s).	*Computing*
· Related Study Programme.	*Electronics and Telecommunications/Introduction to Cybersecurity*
· ISCED Code.	*06 Information and Communication Technologies (ICTs)*
· SDG.	*Goal 4: Quality education, Goal 11: Sustainable cities and communities*
· Study Level.	*Bachelor [B], Masters [M]*

· Number of ECTS credits allocated.	*3*
· Mode of Delivery.	*"Online self-study" + online consultations*
· Language of Instruction.	*English*
· Course Dates.	*01.03.2024 – 31.05.2024*
· Precise Schedule of the Lectures.	*Lectures in "online self-study" mode. Online consultations once a week.*
· Key Words.	*Cybersecurity, network security, network resources, circumvent data, privacy, cryptography, Windows, Linux.*
· Catchy Phrase.	*The course aims to familiarize students with the techniques of monitoring network resources and detecting various types of cyberattacks, network attacks*

· Prerequisites and co-requisites.	*Fundamentals of Computer Networks, English B2* *(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.)*
· Number of EUNICE students that can attend the Course.	*120*
· Course inscription procedure(s).	*Application through the EUNICE website*

2. CONTACT DETAILS.	
· Department.	*Faculty of Computing and Telecommunications*

· Name of Lecturer.	*Prof. Mariusz Głąbowski, D.Sc. Eng; Maciej Sobieraj, D.Sc. Eng*
· E-mail.	*mariusz.glabowski@put.poznan.pl; maciej.sobieraj@put.poznan.pl*
· Other Lecturers.	-

3. COURSE CONTENT.

The course aims to familiarize students with the techniques of monitoring network resources and detecting various types of cyberattacks. It presents techniques used by cybercriminals to circumvent data, privacy, and computer and network security. The students will have the opportunity to familiarize among others with security of Windows and Linux operating systems, as well as with the security of network infrastructure, protocols and services. The course will give a complex view of methods to be used in cybersecurity within IT field.
The course will consist of 15 hours of lectures, 15 hours of labs.
Asynchronous mode: all lectures will be available as recordings; students will have access to laboratory exercises on-line. It is recommended for students to spend 4 hours per week listening to recorded lectures and conducting laboratory exercises.

4. LEARNING OUTCOMES.

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.

5. OBJECTIVES.
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.

6. COURSE ORGANISATION.	
UNITS	
1.	*Cybersecurity vulnerabilities, threats and risks*
2.	*Cybersecurity and the Security Operation Centers*
3.	*Security of Windows operating system*
4.	*Security of Linux operating system*
5.	*Security of network protocols and services*
6.	*Security of network infrastructure*
7.	*Methods for protecting a network*
8.	*Cryptography and the public key infrastructure*
9.	*Endpoint security and analysis*
10.	*Security monitoring*
LEARNING RESOURCES AND TOOLS.	
Virtual course	
PLANNED LEARNING ACTIVITIES AND TEACHING METHODS.	
Lectures, simulation software	

7. ASSESSMENT METHODS, CRITERIA AND PERIOD.
Online Moodle exam
OBSERVATIONS.

8. BIBLIOGRAPHY AND TEACHING MATERIALS.

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