Faculty of Fundamental Problems of Technology

COURSE CARD

Name in polish	:	**Bezpieczeństwo Systemów I**
Name in english	:	**System Security I**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	compulsory
Course code	:	E2_BI01
Group rate	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30	30		
The total number of hours of student workload (CNPS)	60	60	60		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	2	2	2		
including the number of points corresponding to the classes of practical (P)		2	2		
including the number of points corresponding occupations requiring direct contact (BK)	2	2	2		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Basic OS knowledge. Basic computer network knowledge. Programming knowledge.

COURSE OBJECTIVES

C1 Overview of hardware and software conditions related to the security of information systems. Discuss the vulnerabilities resulting from the limitations of the end-user platform, system design, and implementation. Presentation of attack scenarios, detection methods and defense techniques.

C2 Case studies and synthetic examples. Scenarios exercises and pattern best practices.

C3 Master of software and system security testing in selected OS. Acquiring engineering skills in the field of detection / attack. Testing the effectiveness of attacks in a vulnerable virtual environment.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 knows security function and purpose of network devices and software

W2 knows application, data and host security threats and vulnerabilities

W3 knows concepts and practices related to authentication, authorization and access control

The student skills:

U1 can implement security system for a computer network

U2 can implement security system for applications, data, and hosts

U3 can implement security techniques and manage security mechanisms for chosen operating systems

The student's social competence:

K1 can describe and analyse chosen computer security problems in a comprehensive manner.

K2 understands needs of securing computer systems and can argue about it

K3 can use social engineering

COURSE CONTENT

Type of classes - lectures		
Wy1	Definiowanie bezpiecznych funkcjonalności. Definiowanie ataku. Sposoby modelowania adwersarza.	5h
Wy2	Network Security.	8h
Wy3	Realisation errors.	10h
Wy4	Threats and Vulnerabilities.	7h
Type of classes - exercises		
Ćw1	Secure network administration principles. Secure OS administration.	8h
Ćw2	Social engineering attacks. Application attacks.	6h
Ćw3	Practices for authentication, and authorization.	8h
Ćw4	Security controls for account management.	8h
Type of classes - laboratory		
Lab1	Network Security.	10h
Lab2	Threats and Vulnerabilities.	8h
Lab3	Application, Data and Host Security	7h
Lab4	Access Control and Identity Management	5h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Consultation
6. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K3	
F2	U1-U3, K1-K3	
F3	U1-U3, K1-K3	
P=%*F1+50%*F2+50%*F3		

BASIC AND ADDITIONAL READING

1. OWASP Mutillidae II Web Pen-Test Practice Application. https://sourceforge.net/projects/mutillidae/
2. CompTIA Security+ Study Guide: Exam SY0-101
3. Fundamentals of Computer Security
4. Penetration Testing with Kali Linux. https://www.kali.org/

SUPERVISOR OF COURSE

dr inż. Łukasz Krzywiecki

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
System Security I
WITH EFFECTS OF EDUCATION ON THE DIRECTION OF COMPUTER SCIENCE

Course training effect	Reference to the effect of the learning outcomes defined for the field of study and specialization (if applicable)	Objectives of the course**	The contents of the course**	Number of teaching tools**
W1	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W10	C1	Wy1-Wy4	1 2 5 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W10	C1	Wy1-Wy4	1 2 5 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W10	C1	Wy1-Wy4	1 2 5 6
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12	C2 C3	Ćw1-Ćw4 Lab1-Lab4	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2 C3	Ćw1-Ćw4 Lab1-Lab4	3 4 5 6
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2 C3	Ćw1-Ćw4 Lab1-Lab4	3 4 5 6
K1	K2_K02 K2_K03 K2_K05 K2_K06 K2_K07 K2_K09 K2_K10 K2_K12	C1 C2 C3	Wy1-Wy4 Ćw1-Ćw4 Lab1-Lab4	1 2 3 4 5 6
K2	K2_K03 K2_K05 K2_K06 K2_K07 K2_K09 K2_K12	C1 C2 C3	Wy1-Wy4 Ćw1-Ćw4 Lab1-Lab4	1 2 3 4 5 6
K3	K2_K02 K2_K03 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K12	C1 C2 C3	Wy1-Wy4 Ćw1-Ćw4 Lab1-Lab4	1 2 3 4 5 6