Zał. nr 5 do ZW 16/2020

Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Bezpieczeństwo wysokopoziomowe - podatności i ataki**
Name of the course in english	:	**High level security - vulnerabilities and attacks**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	W04INA-SM4009G
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	15	15		
The total number of hours of student workload (CNPS)	60	45	45		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	2	1	1		
including the number of points corresponding to the classes of practical (P)		1	1		
including the number of points corresponding occupations requiring direct contact (BK)	2	1	1		

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, and detection methods.

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 indicate vulnerabilities in IT security components.

U2 can exploit system vulnerabilities and attack faulty security components in IT systems.

U3 can attack badly designed crypto-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
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Synthetic attacks. Threats and Vulnerabilities.	1.0h
Ćw2	Attacks on identification scheme	1.5h
Ćw3	Attacks on privacy.	1.5h
Ćw4	Attacks on anonymity.	1.5h
Ćw5	Attacks on signature schemes.	1.5h
Ćw6	Fault variables and components binding.	1.5h
Ćw7	Fault randomisation usage.	1.0h
Ćw8	Attacks on secrecy.	1.5h
Ćw9	Errors in encryption schemes.	1.5h
Ćw10	Attacks on authenticated key establishment.	1.5h
Ćw11	Attacks based on randomness faults.	1.0h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	Attacks in OSI Application Layer.	1h
Lab2	Bad design vulnerabilities. Social engineering attacks.	1h
Lab3	Web Application attacks. Hacking WebGoat.	1h
Lab4	SQL Injection attacks.	1h
Lab5	Broken Authentication.	2h
Lab6	XML external entities attacks	1h
Lab7	Cross Site Scripting (XSS).	1.5h
Lab8	Insecure deserialization.	1.5h
Lab9	Security misconfiguration.	2h
Lab10	Server-Side Request Forgery (SSRF).	1.5h
Lab11	Timing Attacks.	1.5h
	Sum of hours	15h

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 hab. inż. Łukasz Krzywiecki

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Bezpieczeństwo wysokopoziomowe - podatności i ataki

WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

Subject learning effect	Relating the subject effect to the learning outcomes defined for the field of study	Objectives of the course**	Program content**	Teaching tool number**
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-Ćw11 Lab1-Lab11	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-Ćw11 Lab1-Lab11	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-Ćw11 Lab1-Lab11	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-Wy11 Ćw1-Ćw11 Lab1-Lab11	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-Ćw11 Lab1-Lab11	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-Ćw11 Lab1-Lab11	1 2 3 4 5 6