COURSE DESCRIPTION CARD - SYLLABUS

Course name
Penetration tests [S1Cybez1>TP]

Course

Field of study
Cybersecurity

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
8

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Lecturers

Prerequisites

The student has a well-organized and theoretically grounded knowledge of the functioning of telecommunication networks, including network protocols and services offered within these networks. The student is able to gather information from literature, databases, and other sources; integrate the obtained information, interpret it, draw conclusions, and formulate and justify opinions. The student is capable of working both individually and in a team. The student is aware of the importance of and understands the non-technical aspects and consequences of the activities of an engineer-specialist in the field of cybersecurity, as well as the responsibility associated with the decisions made in this context. They should also understand the necessity of expanding their competencies. Additionally, in terms of social competencies, the student must exhibit attitudes such as honesty, responsibility, perseverance, intellectual curiosity, creativity, personal culture, and respect for others.

Course objective

Presentation of theoretical and practical issues related to penetration testing of computer networks.

Course-related learning outcomes

Knowledge:

The student has advanced and detailed knowledge in the broadly understood field of penetration testing of computer networks. The knowledge includes: 1.Principles of penetration testing,2. Planning and conducting tests (internal and external), 3. Post-test documentation.[K1_W10]
The student is knowledgeable about trends in the development of penetration testing. [K1_W20]

Skills:
The student is able to obtain information about penetration testing and computer networks from literature, databases, and other sources (in Polish and English). [K1_U01]
The student is also capable of integrating knowledge about penetration testing and assessing the usefulness of methods and tools for preparing and conducting tests. [K1_U06]
The student is able to collaborate within a team, assuming various roles and setting directions for further learning. [K1_U15]

Social competences:
The student understands that in the field of computer networks and penetration testing, knowledge and skills quickly become outdated. [K1_K01]
They also understand the importance of using the most up-to-date knowledge.[K1_K02]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired during lectures is verified through a test. The test consists of 30 questions, each offering 4 possible answers, with only one correct answer. The final topics, on the basis of which the questions are prepared, will be sent to students via email using the university's email system.
The knowledge and skills acquired during laboratory exercises are continuously verified by the instructor. Failure to pass an exercise requires it to be repeated at a time designated by the instructor.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

During the lectures, topics related to the planning, execution, and analysis of penetration testing results will be presented. The tests considered will focus on protocols and network devices.
In contrast, during laboratory sessions, students will practice conducting simple tests in practice. These tests will be carried out in a virtual environment or a real network.

Course topics

Lectures:
1. Introduction to Penetration Testing
(Basic definitions, types of penetration testing - white-box, black-box, and gray-box, social engineering techniques, costs and benefits of penetration testing, passive reconnaissance, necessity of penetration testing, stages of penetration testing and client requirements, principles of conduct and risks associated with penetration testing, legal agreements related to penetration testing).
2. Duties of a Licensed Penetration Tester (LPT)
(Professional responsibilities of an LPT, legal standards for LPTs, compliance checklists necessary for conducting penetration tests, rules of cooperation between organizations and penetration testers).
3. Planning and Performing Penetration Tests
(Planning phase of penetration tests, penetration testing team, penetration testing checklist, penetration testing requirements, types of tests, network topology maps, physical location of target servers, various network port scans on the target network, domain DNS records, banners of various servers, ICMP responses, internal network mapping, scanning ports of individual machines, placing viruses, trojans, and rootkits on target machines, Man-in-the-Middle attacks).
4. Information Gathering and Social Engineering Penetration Tests
(Steps in the information-gathering process, social engineering, collecting information about the target company, archived websites).

5. Vulnerability Analysis
(Vulnerability assessment, vulnerability classification, vulnerability assessment report, vulnerability assessment schedule).
6. Penetration Testing Results and Post-Test Activities
(Components of a penetration testing report, how to deliver the report to the client, how long to retain information related to penetration testing, recommendations from the penetration testing team, an action plan for improving security, the process of minimizing misconfiguration cases, conclusions, and best practices).
7. Advanced Exploits and Tools
Laboratory Exercises:
1. Building a Test Environment
2. Pentester Tools
3. Detecting Devices in the Network and Gathering Information
4. Penetration Tests in LAN Networks (Internal Tests)
o Testing network devices
o Testing network protocols
5. Tools for Automatic Vulnerability Detection

Teaching methods

Lecture:
A multimedia presentation supplemented with examples and additional explanations on the board. Lectures are conducted in accordance with the principles of traditional lectures and, in justified cases, in the form of a conversational lecture.
Laboratory Exercises:
A multimedia presentation illustrated with examples provided on the board, along with the execution of tasks assigned by the instructor-practical exercises.

Bibliography

Basic:
Matthew Hickey, Jennifer Arcuri, Warsztat hakera. Testy penetracyjne i inne techniki wykrywania podatności, Helion 2020
Gus Khawaja, Kali Linux i testy penetracyjne. Biblia, Helion 2022
Vijay Kumar Velu, Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV, Helion 2023

Additional:
services on the subject of cyber security, such as www.nist.gov

Breakdown of average student's workload

	Hours	ECTS
Total workload	57	2,00
Classes requiring direct contact with the teacher	32	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	25	1,00