COURSE DESCRIPTION CARD - SYLLABUS

Course name
Information Systems Security Management and Penetration Testing [S2Inf1E-CYB>ISSM]

Course

Field of study Computing	Year/Semester 2/3
Area of study (specialization) Cybersecurity	Profile of study general academic
Level of study second-cycle	Course offered in English
Form of study full-time	Requirements compulsory

Number of hours

Lecture 30	Laboratory classes 30	Other 0
Tutorials 0	Projects/seminars 30	

Number of credit points

6,00

Coordinators

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

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

dr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl

Lecturers

Prerequisites

The student has structured and theoretically founded knowledge of the architecture of computer systems, the principles of operation of operating systems and their types, knows and understands the basic processes occurring in the life cycle of the IT systems. The student has an structured and theoretically founded knowledge of the basics of ICT, protocols and services in telecommunications networks. The student knows the basics of data protection in the information system. The student is able to obtain information from literature, databases and other sources; is able to integrate the obtained information, interpret it, as well as draw conclusions and formulate and justify opinions. The student is able to work individually and cooperate in a team. The student is aware of the importance and understands the non-technical aspects and effects of the activity of an IT engineer and the related responsibility for the decisions made. He should also understand the need to expand his competences. In addition, in terms of social competences, the student must present attitudes such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

As part of the course, students learn about the issues of ICT security management in a company or institution, i.e. based on norms and standards, methods of risk analysis and appropriate selection of security (minimizing the probability and / or effects of threats), methods of responding to incidents and restoring the system information technology to the state before the incident.

Course-related learning outcomes

Knowledge:
a student has structured and theoretically founded knowledge in the field of data protection, security of it systems, risk analysis, has basic knowledge in the field of it systems administration and is aware of the obligations of information system administrators.
a student has advanced and detailed knowledge of the widely understood penetration tests of computer networks. the knowledge includes:
1. principles of penetration tests
2. planning and conducting tests (internal and external),
3. post-tests documentation.
the student has knowledge about development trends of penetration tests and computer networks. preparing and conducting tests. he also is able to interact in a team, taking various roles in it and can determine the directions of further learning.

Skills:
a student can apply appropriate data protection methods and ensure the security of the it system, can prepare documentation on the implementation of an engineering task and prepare a text containing a discussion of the results of this task, can make a critical analysis of existing solutions.
the student is able to obtain information about penetration tests and computer networks from literature, databases and other sources (both in polish and english). the student can also integrate

Social competences:
a student understands that in it and penetration tests knowledge and skills very quickly become obsolete, especially technologies related to security,
a student is aware of the importance and understands the non-technical aspects and effects of the activity of an it engineer and the related responsibility for the decisions made.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Lecture - the knowledge acquired during the lectures is verified during the test, oral or in writing. The test passing threshold is 50%. The correctness of the answers and the student''s understanding of the problem are assessed. Final issues on the basis of which questions are prepared will be sent to students by e-mail using the university e-mail system. In the case of the oral exam, each student answers three questions from the set of 40 (they are known to students).
Project - based on the assessment of the current progress in the implementation of tasks.
Knowledge and skills acquired during laboratory exercises are verified by checking the correctness of the exercise. Lack of passing the exercise results in the need to repeat it within the time limit indicated by the teacher

Programme content

Course Content:
Risk Analysis. Security Rules. Vulnerability Analysis. Threat Analysis and Modeling. Penetration Testing

Course topics

The lecture program covers the following issues:
Introduction - the definition of what it means that the IT system is a safe and reliable system, how to assess security, relationships between security elements, standards, measures, norms and best practices (TCSEC, ITSEC, ISO, CC). Classification of threats, both network, cryptographic and computer systems expoits. Determining the degree of systems'' vulnerability (quantitative and qualitative methods). Risk

analysis and management. Defining and discussing ways to achieve and maintain the assumed level of confidentiality, integrity, availability, accountability, authenticity and reliability. Selection of appropriate precautionary measures. Examples of risk management processes in a company in a specific IT system. Security policy - sample documents included in a security policy. Audit - an example of an implementation of a security management system (COBIT, MARION, TISM, OSSTM, LP-A). Models of trust systems (flat, hierarchical, decentralized, user-oriented). Trust issues (cognitive biases). Implementation of trust models (including in PKI systems). Models of choosing the security strategy (security by obscurity, open security) Legal requirements related to security management. The human factor problem in data protection. Economic aspects of security in IT systems (financial consequences of security breaches, cost of security). Supporting users of information systems. Organization of training in the field of data protection. Rules for the editing of instructions for use. Mnemonics in password systems. IT tools supporting security management processes, including the use of artificial intelligence in data protection. Penetration testing methodologies (introduction to penetration testing, basic definitions, types of penetration tests - white-, black-, and gray-box , social-engineering techniques, costs and benefits of a
penetration test, passive reconnaissance). Customers and legal agreements (the need for penetration testing, stages of penetration testing, and customer requirements, the rules of behavior and risks associated with penetration testing, legal agreements involved in penetration testing). Duties of a Licensed Penetration Tester (LPT) (professional duties of an LPT, legal standards for an LPT, compliance checklists necessary for conducting a penetration test, rules of engagement (ROE) between an organization and penetration testers) Penetration testing planning and scheduling (penetration testing planning phase, penetration testing team) Pre–penetration testing checklist (pre penetration testing checklist, penetration testing requirements, types of testing that will be carried out during the penetration test) Information Gathering and Social Engineering Penetration Testing (steps in the information-gathering process, social engineering, gathering information about a target company, archive pages) Vulnerability Analysis (vulnerability assessment, classification of vulnerabilities, vulnerability assessment report, timeline for a vulnerability assessment) External Penetration Testing (topological network maps, the physical location of target servers, variety of port scans on a target network, DNS record of a domain, banners of a variety of servers, ICMP responses)
Internal Network Penetration Testing (mapping of an internal network, port-scan individual machines, planting viruses, Trojans, and rootkits on a target machine, MitM) Penetration Testing Deliverables (the components of a penetration testing report, how to deliver the report to the client, how long to retain information related to a penetration test) Post-Testing Actions (recommendations of a penetration testing team, action plan for improving security, process for minimizing instances of misconfigurations, lessons learned and the best practices) Advanced Exploits and Tools

Laboratories / project
Development of the design and documentation of the security management system in the selected IT environment, taking into account: hardware and software IT resources, type of processed data, risk analysis with a proposal of changes, post-implementation analysis.Educational methods used: work in teams of up to 2 persons, presentations of the progress of work on the system documentation, discussions on the proposed solutions in the forum of the whole group and individually with the team

Laboratory exercises
1. Preparation of the tester''s environment - Kali Linux virtual machine (Virtual Box)
2. Passive gathering of information about the test object (DNS, Google hacking, Archive.org, social engineering)
3. Scanning: networks and devices (scanning technics, optimal techniques from the point of view of e.g. their detection by IDS / IPS systems, tests of chosen scanning techniques, tools)
4. Tests of Web applications (technics, tools)
5. Internal network penetration testing
6. External penetration testing
7. Preparation of complete network tests scenarios
8. Conducting planned tests in a laboratory environment
9. Preparation of documentation after the tests performed

Teaching methods

Lecture: lecture conducted in an interactive way with the formulation of questions to a group of students or to specific students indicated, the activity of students during classes is taken into account when giving the final grade, initiating a discussion during the lecture.

Project: project - detailed review of project documentation by the project leader and discussions on comments, work in two-person teams
Laboratory exercises: multimedia presentation, presentation illustrated with examples given on a blackboard, and performance of tasks given by the teacher - practical exercises.

Bibliography

Basic
1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A. WNT, Warszawa 2017.
2. Bezpieczeństwo informacyjne : nowe wyzwania, Liderman K, PWN Warszawa 2017.
3. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, NIST 800-37 rev.2, 2018
4. EC-Council, Penetration Testing: Procedures & Methodologies, Cengage Learning 2011
5. Wnag J., Computer network security : theory and practice, Higher Education Press 2009.
6. Tanenbaum A. S., Wetherall D. J., Computer networks, Pearson Longman 2014 .
Additional
1. Normy ISO (13335, 2700x),
2. Audyt bezpieczeństwa systemów IT-ścieżka techniczna (rekonesans i skanowanie), Księżopolski B., Szałachowski P., Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin, 2011.
3. www.cisco.com

Breakdown of average student's workload

	Hours	ECTS
Total workload	150	6,00
Classes requiring direct contact with the teacher	90	3,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	60	2,50