Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației

COURSE DESCRIPTION

1. Program identification information

1.1 Higher education institution	**National University of Science and Technology Politehnica Bucharest**
1.2 Faculty	**Electronics, Telecommunications and Information Technology**
1.3 Department	**Telecommunications**
1.4 Domain of studies	Electronic Engineering, Telecommunications and Information Technology
1.5 Cycle of studies	Masters
1.6 Programme of studies	Services and Network Management

2. Date despre disciplină

2.1 Course name (ro) (en)				Managementul securității rețelelor și serviciilor			
2.2 Course Lecturer				S.l./Lect. Dr. Laurentiu BOICESCU			
2.3 Instructor for practical activities				S.l./Lect. Dr. Laurentiu BOICESCU			
2.4 Year of studies	1	2.5 Semester	II	2.6. Evaluation type	E	2.7 Course regime	Ob
2.8 Course type		DA	2.9 Course code	UPB.04.M2.O.11-15		2.10 Tipul de notare	Nota

3. Total estimated time (hours per semester for academic activities)

3.1 Number of hours per week	3	Out of which: 3.2 course	2.00	3.3 seminary/laboratory	1
3.4 Total hours in the curricula	42.00	Out of which: 3.5 course	28	3.6 seminary/laboratory	14
Distribution of time:					hours
Study according to the manual, course support, bibliography and hand notes Supplemental documentation (library, electronic access resources, in the field, etc) Preparation for practical activities, homework, essays, portfolios, etc.					54
Tutoring					0
Examinations					4
Other activities (if any):					0

3.7 Total hours of individual study	58.00
3.8 Total hours per semester	100
3.9 Number of ECTS credit points	4

4. Prerequisites (if applicable) (where applicable)

4.1 Curriculum	Computer Programming Communications Architectures and Protocols Communications Networks Architectures for Networks and Services
4.2 Results of learning	Knowledge regarding communications networks

5. Necessary conditions for the optimal development of teaching activities (where applicable)

5.1 Course	In accordance with the university internal rules The lectures will take place in a room equipped with computer and video projector
5.2 Seminary/ Laboratory/Project	The laboratories will take place in a room equipped with video projector, computers with NetBeans IDE, web-server (Apache Tomcat), Database server (MySQL), virtual machine hypervisor (VirtualBox)

6. General objective *(Reffering to the teachers' intentions for students and to what the students will be thought during the course. It offers an idea on the position of course in the scientific domain, as well as the role it has for the study programme. The course topics, the justification of including the course in the currcula of the study programme, etc. will be described in a general manner)*

The course aims at the familizarization of studentis with basic knowledge on communications networks and information security management, as well as the main vulnerabilities, attacks and protection mechanisms, as well as acquiring the ability to analyze the security level of a network and to design protection systems for information, computers and communications networks.
Specific objectives include: completion of student training in advanced software (and hardware) technologies for communications networks and information protection, acquiring the knowledge needed to test and evaluate network security, acquiring the knowledge required to design advanced multilayered systems for the protection of communications networks.

7. Competences *(Proven capacity to use knowledge, aptitudes and personal, social and/or methodological abilities in work or study situations and for personal and proffesional growth. They refflect the empolyers requirements.)*

Specific Competences	Operating with scientific, engineering and information security management foundations The application of basic knowledge, concepts and methods for the security management of communication networks The use of programming languages and specialized software tools for the security management of information and communication networks
Transversal (General) Competences	The methodical analysis of the daily issues, identifying the problems for which well-known solutions are already available, thus accomplishing the professional tasks Accommodation to new technologies, personal and professional development, through continuous training using printed documentation, specialized software and digital resources in Romanian and, at least, one international language

8. Learning outcomes *(Synthetic descriptions for what a student will be capable of doing or showing at the completion of a course. The learning outcomes reflect the student's acomplishments and to a lesser extent the teachers' intentions. The learning outcomes inform the students of what is expected from them with respect to performance and to obtain the desired grades and ECTS points. They are defined in concise terms, using verbs similar to the examples below and indicate what will be required for evaluation. The*

learning outcomes will be formulated so that the correlation with the competences defined in section 7 is highlighted.)

Knowledge	*The result of knowledge aquisition through learning. The knowledge represents the totality of facts, priciples, theories and practices for a given work or study field. They can be theoretical and/or factual.* **main** hardware and software mechanisms used in the field (access control systems, intrusion detection and prevention systems, network security testing and evaluation tools) **main mechanisms for ensuring the confidentiality of information (symmetric and asymmetric cryptography, public key infrastructure)** **architectural models used** for the security of networks and services
Skills	*The capacity to apply the knowledge and use the know-how for completing tasks and solving problems. The skills are described as being cognitive (requiring the use of logical, intuitive and creative thinking) or practical (implying manual dexterity and the use of methods, materials, tools and intrumentation).* Uses principles that are specific to the security of networks and services and motivates the choices Works in a team Elaborates scientific text Verifies identified solutions through experiment Solves practical applications Analyses and compares network and service security technologies and libraries Identifies solutions and develops solution plans/projects Motivates the identified solutions
Responsability and autonomy	*The student's capacity to autonomously and responsably apply their knowledge and skills.* Respects academic ethics principles, correctly citing the bibliographic sources used. Is receptive to new learning contexts. Collaborates with peers and teachers in carrying out course activities Shows autonomy in managing the learning/problem solving situation/context Awareness of the value of the contribution to identifying a viable / sustainable solution to solve problems in social and economic life (social responsibility). Analyses and capitalizes on business opportunities in the specializes field. Demonstrates skills in managing real-life situations (time management, collaboration, conflict).

9. Teaching techniques *(Student centric techniques will be considered. The means for students to participate in defining their own study path, the identification of eventual fallbacks and the remedial measures that will be adopted in those cases will be described.)*

Starting from the analysis of students' learning patterns and their specific needs, the teaching process will explore both presentational (lecture, presentation) and conversational-interactive teaching methods, based on discovery and exploration models (experimentation, demonstration, modeling), as well as using exercises, practical activities and problem solving.
Lectures based on Power Point presentations (that will be made available to students) will be used in the teaching activity. Each course will begin with a recap of the chapters already covered, with an emphasis on the concepts covered in the previous course. The first lectures will recap the object-oriented notions studied during the previous semesters.
Presentations rely on images and diagrams, making the information of the lectures easy to understand and assimilate.
This course offers information and practical activities meant to aid th students in their efforts to learn and

develop optimal collaborative an communicational relationship in a climate suitable to learning through discovery.
The ability for teamwork in solving different learning assignments will be encouraged.

10. Contents

COURSE		
Chapter	**Content**	**No. hours**
1	General notions on communications networks and information security General notions Information security Security mechanisms	2
2	Vulnerabilities and attacks on communications networks and services Vulnerabilities of the main operations systems and communication technologies Attacks on communication systems and protocols. "Zero-Day" attacks. Identifying the vulnerabilities of computers and computer networks. Vulnerability databases	4
3	Information security. Cryptography. General notions Vulnerabilities and attacks on cryptographic systems Classes of cryptographic systems Symmetric and asymmetric cryptography Cryptographic certificates Digital signature Public Key Infrastructure	8
4	Hardware and software technologies for protecting computers and software services. The principles of securing computers. The principle of layered security. Hardware and software authentication systems. Biometric systems. Advanced technologies. Security coprocessors. TPM (Trusted Platform Module). Linux security Web service security	6
5	Telecommunications networks security management The principle of layered security in communications networks. Demilitarized zones. IDS/IPS systems and firewalls; network traffic fingerprinting and attack identifying methods Studying and hijacking attacks with Honeypots Network security management systems. The security information and event management.	6
6	Authentication, Authorization and Accounting (AAA) mechanisms. The principles of AAA systems Well-known AAA systems. The Radius protocol and server Wireless Network Security (WLAN 802.11)	2
	Total:	28

Bibliography:
Course notes, available on the Moodle platform
"Information security management handbook", 6th edition, Auerbach publications, 2007, ISBN: 978-0-8493-7495-1
"Computer and Information Security Handbook", Morgan Kaufmann Publishers, 2009, ISBN: 978-0-12-374354-1
"Hardware based computer security techniques to defeat hackers", John Wiley and Sons, 2008, ISBN: 978-0-470-19339-6
W. Stallings, L. Brown, "Computer Security: Principles and Practice (2nd Edition)", Prentice Hall, 2008, ISBN: 978-0-13-277506-9
A. J. Menezes, P. C. van Oorschot; S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996, ISBN: 0-8493-8523-7
B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C" (20th Anniversary Edition), Wiley, 2015, ISBN: 978-1-119-09672-6
W. Stallings, "Cryptography and Network Security" (4th Edition), Prentice Hall, 2005, 978-0-13-187316-2
D. Littlejohn Shinder, M. Cross, "Scene of the Cybercrime" 2nd edition, Syngress Publishing, Elsevier, 2008, ISBN: 978-1-59749-276-8
V. Patriciu, M. Ene-Pietroşanu, I. Bica, I. Priescu, "Semnaturi electronice si securitate informatica", Bic All, 2006, ISBN: 973-571-564-3
K. Scarfone, W. Jansen, M. Tracy , "Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology, 2008, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
G. Stoneburner, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems", NIST SP 800-30, July 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
ISECOM, „Open Source Security Testing Methodology Manual (OSSTMM)", www.isecom.org/mirror/OSSTMM.3.pdf

LABORATORY

Crt. no.	Content	No. hours
1	Public key management Familizarization with the Linux operating system Public Key Management PKI infrastructure Practical applications of cryptographic certificates. HTTPs	4
2	Detecting attacks on TCP/IP networks Traffic filtering mechanisms. Firewall systems Intrusion detection and prevention systems Security information and events management	4
3	Vulnerability management Network Security Testing Mechanisms. Identifying vulnerabilities and threats to telecommunication networks	4
4	Final Laboratory Examination	2
	Total:	14

Bibliography:
See the above.
Laboratory guide, available on the Moodle platform

11. Evaluation

Activity type	11.1 Evaluation criteria	11.2 Evaluation methods	11.3 Percentage of final grade
11.4 Course	- knowledge of fundamental theoretical notions; - knowing how to apply the theory to specific problems; - analysis of theoretical techniques and methods.	Verification during the semester at dates fixed at the beginning of the semester. Final verification during the session.	50%
11.5 Seminary/laboratory/project	- development of the skills for configurating, implementing and operating security management mechanisms and systems	Final laboratory test comprising a theoretical and a practical component, checking the way the student solves a practical problem (implementation, testing, operation).	30%
	Homework: - the ability to analyze and synthesize on the topic at hand - the ability to implement the practical application, as required - the ability to present and argue on the practical implementation	Final project presentation	20%
11.6 Passing conditions			
Obtaining 50% of the total score. Obtaining a 50% of the score related to activities during the semester.			

12. Corroborate the content of the course with the expectations of representatives of employers and representative professional associations in the field of the program, as well as with the current state of knowledge in the scientific field approached and practices in higher education institutions in the European Higher Education Area (EHEA)

Through their activity, students gain the ability to provide solutions to existing problems and propose ideas to improve the current situation in the field of telecommunication networks and services security.
The development of the lecture relied on knowledge, theoretical an practical aspects as well as phenomena described by the specialized literature, own published research and the experience of the lecturers.
The course aims to develop the graduates' skills to design and implement new security mechanisms, as well as to analyse, debug and improve existing ones. Thus, graduates of the course can contribute to the economic environment, in the field of networks' security.

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

Date	Course lecturer	Instructor(s) for practical activities
	S.l./Lect. Dr. Laurentiu BOICESCU	S.l./Lect. Dr. Laurentiu BOICESCU

Date of department approval	Head of department
27.10.2024	Conf. Dr. Serban Georgica Obreja

Date of approval in the Faculty Council	Dean
01.11.2024	Prof. Dr. Mihnea Udrea