SYLLABUS

1. Data about the program of study

1.1	Institution	Technical University of Cluj-Napoca
1.2	Faculty	Electronics, Telecommunications and Information Technology
1.3	Department	Communications
1.4	Field of study	Electronics and Telecommunications Engineering
1.5	Cycle of study	Master of Science
1.6	Program of study/Qualification	Telecommunications/ Multimedia Technologies
1.7	Form of education	Full time
1.8	Subject code	TC-E17.30

2. Data about the subject

2.1	Subject name					Security of IT Systems					
2.2	Subject area					Electronics and Telecommunications Engineering					
2.3	Course responsible/lecturer					Assistant Professor Tudor Mihai BLAGA, PhD					
2.4	Teachers in charge of applications					Assistant Professor Tudor Mihai BLAGA, PhD					
2.5	Year of study	II	2.6	Semester	1	2.7	Assessment	Exam	2.8	Subject category	DS/DO

3. Estimated total time

Year/ Sem.	Subject name	No. of weeks	Course	Applications			Course	Applications			Indiv. study	TOTAL	Credits
			[hours/ week]				[hours/ semester]						
				S	L	P		S	L	P			
II/1	Security of IT Systems	14	2	0	1	0	28	0	14	0	58	100	4

3.1	Number of hours per week	3	3.2	of which, course	2	3.3	applications	1
3.4	Total hours in the curriculum	42	3.5	of which, course	28	3.6	applications	14

Individual study	Hours
Manual, lecture material and notes, bibliography	16
Supplementary study in the library, online and in the field	8
Preparation for seminars/laboratory works, homework, reports, portfolios, essays	14
Tutoring	2
Exams and tests	3
Other activities	15

3.7	Total hours of individual study	58
3.8	Total hours per semester	100
3.9	Number of credit points	4

4. Pre-requisites (where appropriate)

4.1	Curriculum	Computer Networks, Internet Protocols, Switching and routing systems.
4.2	Competence	No

5. Requirements (where appropriate)

5.1	For the course	No
5.2	For the applications	TUCN

6. Specific competences

Professional competences	Upon completion of the course students will know: - Principles of security in IT systems (CIA – Confidentiality, Integrity, Availability) - Approach: Prevention, Detection and Response - Incident handling steps and response - Secure network architecture – basics - Security standards for Linux & Public Cloud - Web Applications Security – basics - Malware analysis and prevention & detection mechanisms - Risk Management principles - Security Training & Awareness Upon completions of the course students will be able to: - Configure basic security features for Linux systems - Configure basic security features for public cloud (AWS) - Assess security of a web applications using specific vulnerability testing tooling - Assess the security risk of an IT systems (impact and likelihood) - Assess the security posture of a network architecture
Cross competences	CT 6 - Ability to integrate into the organization's management team

7. Discipline objectives (as results from the key competences gained)

7.1	General objectives	Developing the competences regarding the use, analysis and design in the field of Information Security
7.2	Specific objectives	1. Understanding fundamental principles for security of IT systems and web applications. 2. Build capabilities needed to implement, assess and test the security of IT systems

8. Contents

8.1. Lecture (syllabus)		Teaching methods	Notes
1	Introduction to Information Security	Presentation, heuristic conversation, exemplification, problem presentation, teaching exercise, case study, formative evaluation	Use of .ppt presentation, projector, blackboard
2	Defence-in-Depth		
3	Incident Handling Foundations		
4	Principles of Secure Network Design		
5	Security of Public Cloud (AWS)		
6	Security of Public Cloud (AWS)		
7	Security of Unix/Linux Systems 1		
8	Security of Unix/Linux Systems 2		
9	Security of Web Applications 1		
10	Security of Web Applications 2		
11	Malware Analysis		
12	Risk Management		
13	Information Security Management System ISO27001		
14	Recap, exam preparation		

8.2. Applications (lab)		Teaching methods	Notes
1	Introduction to Laboratory Activities	Didactic and experimental proof, didactic exercise, team work	Use specific security tools or virtual machines.
2	Security Awareness Program		
3	Creating a Security Awareness Program 1 (mini-project)		
4	Creating a Security Awareness Program 2 (mini-project)		
5	Security of Windows Systems 1		
6	Security of Windows Systems 2		
7	Security of Unix/Linux Systems 1		
8	Security of Unix/Linux Systems 2		
9	Tools for Pentesting Web Applications: Burp, Accunetix		
10	Exploiting Web Application Vulnerabilities		
11	Malware Analysis		
12	Risk Assessment: impact and probability		
13	Mini-project Presentation		
14	Laboratory Recovery		

Bibliography

1. Peter Kim, „The Hacker Playbook: Practical Guide To Penetration Testing", CreateSpace, 2014
2. Patrick Engebretson, „The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy", Syngress, 2nd edition, 2013
3. Daniel Dieterle, „Basic Security Testing with Kali Linux", CreateSpace, 2014
4. Eric Cole - „Network Security Bible", Wiley, 2009
5. Dafydd Stuttard & Marcus Pinto, „The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley, 2nd edition, 2011

On-line references

1. T. Blaga, Security of IT Systems. Technical University of Cluj-Napoca, 2018 http://users.utcluj.ro/~tblaga/ssit/

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

Competences acquired will be used in the following COR occupations (banking security system administrator, security consultant, security director, security systems engineer, information security manager, information security officer)

10. Evaluations

Activity type	10.1	Assessment criteria	10.2	Assessment methods	10.3	Weight in the final grade
Course		The level of acquired theoretical knowledge and practical skills		Written exam – multiple choice test		50%
Applications		The level of acquired abilities		Oral presentation on building a Security Awareness program		50%
10.4 Minimum standard of performance						
Written exam grade at least 5 (out of 10), Application grade at least 5 (out of 10)						

Date of filling in
1.10.2018

Course responsible
Assistant Professor
Tudor Mihai BLAGA, PhD

Teachers in charge of applications
Assistant Professor
Tudor Mihai Blaga, PhD

Date of approval in the department
1.10.2018

Head of Communications Department
Professor Virgil DOBROTA, PhD