SYLLABUS

1. Information regarding the programme

1.1 Higher education institution	**Babeș-Bolyai University**
1.2 Faculty	**Faculty of Mathematics and Computer Science**
1.3 Department	**Computer Science Department**
1.4 Field of study	**Computer Science**
1.5 Study cycle	**Master**
1.6 Study programme / Qualification	**Cyber Security**

2. Information regarding the discipline

2.1 Name of the discipline (en) (ro)			**Web and Internet Security / Securitate Web și în Internet**				
2.2 Course coordinator			**Assoc. Prof. Bufnea Darius-Vasile**				
2.3 Seminar coordinator			**Assoc. Prof. Bufnea Darius-Vasile**				
2.4. Year of study	**1**	2.5 Semester	**2**	2.6. Type of evaluation	**E**	2.7 Type of discipline	**Mandatory**
2.8 Code of the discipline		**MME8194**					

3. Total estimated time (hours/semester of didactic activities)

3.1 Hours per week	4	Of which: 3.2 course	2	3.3 seminar/laboratory	1 sem + 1 pr
3.4 Total hours in the curriculum	56	Of which: 3.5 course	28	3.6 seminar/laboratory	28
Time allotment:					hours
Learning using manual, course support, bibliography, course notes					25
Additional documentation (in libraries, on electronic platforms, field documentation)					25
Preparation for seminars/labs, homework, papers, portfolios and essays					20
Tutorship					14
Evaluations					10
Other activities:					0

3.7 Total individual study hours	94
3.8 Total hours per semester	150
3.9 Number of ECTS credits	6

4. Prerequisites (if necessary)

4.1. curriculum	• • Computer Architecture, Operating Systems, Computer Networks, Web Programming, Modular Arithmetic and Cryptography
4.2. competencies	• Basic knowledge of the structure and operation of the Internet,

	basic knowledge of cryptography, operating systems, computer architecture, databases, web programming, client-server model, algorithm and programming

5. Conditions (if necessary)

5.1. for the course	• Classroom equipped with video projector
5.2. for the seminar /lab activities	• None

6. Specific competencies acquired

Professional competencies	Professional competencies • Know and understand the main paradigms related to data protection: confidentiality, integrity and data availability; • Acquiring a solid theoretical foundation in communication through unsafe medium, as well as the use of secure communication protocols on the Internet; • Learning how the main forms of malware and the main forms of attacks on the Internet work, as well as the methods of protection against them.
Transversal competencies	• Professional communication skills; concise and precise description, both oral and written, of professional results; • Ethic and fair behaviour, commitment to professional deontology; • Applying the norms of organized and efficient work, responsibility and reliability of the work performed both individually and within a team; • Entrepreneurial skills; working with economical knowledge; continuous learning; • Good English communication skills.

7. Objectives of the discipline (outcome of the acquired competencies)

7.1 General objective of the discipline	The course aims to deepen the student's knowledge of the best security mechanisms that can be implemented and used on the Internet, both at the level of a computer system and at the level of the communication infrastructure.
7.2 Specific objective of the discipline	The course brings together some advanced topics in the field of cyber security. The course is structured around the TCP / IP architecture for organizing computer networks, the theoretical aspects being oriented towards each level and set of protocols within the TCP / IP stack. The course aims to: • present and familiarize the student with the most common encryption algorithms as well as with the different protocols at various levels in the TCP / IP stack that implement these algorithms; • a comprehensive presentation of the main aspects of cryptography applied on the Internet, in particular of public and private key cryptography; • familiarize the student with the most serious vulnerabilities in the field, as well as with the mechanisms and measures to combat these vulnerabilities;

	• present to students the main security challenges posed by e-commerce on the Internet; • address from a legal and moral point of view various topics such as Internet crime and user privacy; • contribute to the understanding of these fields by studying and developing relevant practical applications.

8. Content

8.1 Course	Teaching methods	Remarks
1. Presentation of the bibliography and the structure of the course. Requirements and evaluation. Computer vulnerabilities. Policies and aspects of IT security at different levels of the TCP / IP stack.	Presentations, explanations, examples, case studies	
2. History of computer attacks. Malware (classification). Computer virology. The anatomy of a computer virus. Antivirus systems. Spyware and addware. Their applications in e-commerce. Botnet networks.	Presentations, explanations, examples, case studies	
3. Computer vulnerabilities. Operating system security.	Presentations, explanations, examples, case studies	
4. Internet server security. Enterprise network security architectures.	Presentations, explanations, examples, case studies	
5. Local area network security. Firewall mechanism (host based, router based). Network & host scanning. Types of scans.	Presentations, explanations, examples, case studies	
6. Local attacks and remote attacks. Escalation of privileges. Horizontal attacks. DDOS, flood.	Presentations, explanations, examples, case studies	
7. Buffer overflow. Exploits' anatomy. Shellcode.	Presentations, explanations, examples, case studies	
8. Web application security. SQL Injection. SMTP Injection. Cross Site Scripting. CSRF. Unrestricted file upload.	Presentations, explanations, examples, case studies	
9. Encryption algorithms based on public and private keys. Digital signatures. Digital certificates.	Presentations, explanations, examples, case studies	
10. Public keys infrastructures and associated services.	Presentations, explanations, examples, case studies	
11. E-mail security. DKIM. Antispam mechanism: bayesian spam filters, DNS based blacklists. PGP.	Presentations, explanations, examples, case studies	
12. Network and transport security protocols. IPSec. SSL and TLS. VPN	Presentations, explanations, examples, case studies	
13. Physical and data link layer security	Presentations, explanations, examples, case studies	
14. Social Engineering related vulnerabilities. Cyber crime. Ensuring user privacy.	Presentations, explanations, examples, case studies	

Bibliography

1. F. Cohen, A Short Course on Computer Viruses, Wiley Professional Computing, 2nd edition, 1994
2. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012
3. Peter Kim, The Hacker Playbook 2: Practical Guide To Penetration Testing, CreateSpace, 2015
4. Martin Boldt, Privacy-Invasive Software, cap. 2, cap. 7, Blekinge Institute of Technology, ISBN 978-91-7295-100-6
5. Michal Zalewski, Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks, No Starch Press, 2005
6. Michael Hale Ligh, Andrew Case, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, John Wiley & Sons, 2014
7. Chris Sanders, Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis,

Syngress, 2013
8. Shon Harris, Allen Harper, Gray Hat Hacking, Second Edition: The Ethical Hacker's Handbook, McGraw-Hill Osborne, 2008
9. Michal Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, No Starch Press, 2011
10. Michael A. Davis and Sean M. Bodmer, Hacking Exposed Malware and Rootkits: Malware and Rootkits Secrets and Solutions, McGraw-Hill Education, 2009
11. Michael Gregg, The Network Security Test Lab: A Step-by-Step Guide, John Wiley & Sons, 2015
12. William Stallings, Network Security Essentials: Applications and Standards, Pearson, 5th edition, 2013
13. Stuart Mcclure, Joel Scambray, Hacking Exposed 7: Network Security Secrets and Solutions, McGraw-Hill Education, 7th edition, 2012
14. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 6th edition 2013
15. Gordon Fyodor Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Nmap Project, 2009
16. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2002
17. Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollmann, Rachelle Reese, Network Security Fundamentals, John Wiley & Sons, 2008
18. Michael J. Stewart, Network Security, Firewalls and VPNs, Jones & Bartlett Learning, 2nd edition, 2013
19. Timur Mehmet, Firewall Hacking Secrets For Security Professionals, HackerStorm, 2015
20. Oskar Andreasson, Iptables Tutorial, http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
21. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, John Wiley & Sons, 2nd edition, 2011
22. Jon Erickson, Hacking: The Art of Exploitation, No Starch Press, 2nd edition, 2008
23. Vancea, Al. si altii, Programarea in limbaj de asamblare 80x86, Exemple si aplicatii, pag. 317-323, Ed. Risoprint, 2005
24. Klaus Schmeh, Cryptography and Public Key Infrastructure on the Internet, Wiley, 2007
25. Johannes A. Buchmann, Evangelos Karatsiolis, Introduction to Public Key Infrastructures, Springer, 2013
26. V. V. Patriciu, M. Ene-Pietrosanu, C. Vaduva, I. Bica, N. Voicu, Securitatea Comerţului Electronic, Editura ALL
27. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnături Electronice şi Securitate Informatică, Editura ALL, 2006
28. Sharon Conheady, Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques, McGraw-Hill Education, 2014
29. Christopher Hadnagy, Paul Wilson, Social Engineering: The Art of Human Hacking, John Wiley & Sons, 2010

8.2 Seminar / laboratory	Teaching methods	Remarks
1. Computer vulnerabilities. Computer virology. The anatomy of a computer virus. Antivirus systems.	Debate, dialogue, examples, conversations	The seminar takes place every two weeks
2. Exploits. Shell-code.	Debate, dialogue, examples, conversations	
3. Firewalls	Debate, dialogue, examples, conversations	
4. Web applications security	Debate, dialogue, examples, conversations	
5. Public key encryption algorithms. Digital signatures. Digital certificates.	Debate, dialogue, examples, conversations	

6. E-mail security	Debate, dialogue, examples, conversations	
7. Network and transport layers security protocols.	Debate, dialogue, examples, conversations	

Bibliography

1. Justin Pot: A History of Computer Viruses & The Worst Ones of Today;
2. Jeremy Paquette: A History of Viruses;
3. Moheeb Abu Rajab, Lucas Ballard, Panayiotis Mavrommatis, Niels Provos, Xin Zhao: The Nocebo* Effect on theWeb: An Analysis of Fake Anti-Virus Distribution;
4. Martin Boldt: Privacy-Invasive Software, cap. 2, cap. 7;
5. Steve Hanna: Shellcoding for Linux and Windows Tutorial;
6. Writing shellcode;
7. Lisa Bogar: SUID, SGID;
8. Vivek Gite, Explain Linux / UNIX TCP Wrappers, 2009;
9. Port Scanning – How a Port Scan Works;
10. James Messer: Secrets of Network Cartography: A Comprehensive Guide to nmap;
11. TCP Idle Scan;
12. V. V. Patriciu: Semnaturi electronice si infrastructuri de securitate, notiţe de curs, 2009, Master Sisteme Distribuite în Internet, Univ. Babeş-Bolyai;
13. DomainKeys Identified Mail (DKIM);
14. OpenSSL: The Open Source toolkit for SSL/TLS, www.openssl.org;
15. Steve Friedl: An Illustrated Guide to IPsec.

9. Corroborating the content of the discipline with the expectations of the epistemic community, professional associations and representative employers within the field of the program

Courses with a similar content exist in the curriculum of all major universities in Romania and abroad.

• The course addresses fundamental security issues and especially current ones on the Internet.
• The content of the course covers the main aspects necessary to be mastered by the student in order to successfully occupy a suitable position within a profile company.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Share in the grade (%)
10.4 Course	Knowledge of the main theoretical aspects presented in the course	Partial examination of the first half of the curriculum	1/4
	Knowledge of the main theoretical aspects presented in the course	Final exam in the second half of the curriculum	1/4
10.5 Seminar/lab activities	Delivery of reports and projects on security topics chosen by mutual agreement of the student with the teacher (among those discussed at the course and/or seminar)	Oral presentation by the student	1/2
10.6 Minimum performance standards			
The following two conditions must be met for the student to pass the course: • semester-long activity (presentation of reports and projects), activity that must be noted at least with a			

grade of 5;
• minimum average 5 between the mark of the partial exam and the one obtained at the exam in the evaluation session.

Date	Signature of course coordinator	Signature of seminar coordinator
.....	Assoc. Prof. Bufnea Darius-Vasile	Assoc. Prof. Bufnea Darius-Vasile

Date of approval	Signature of the head of department
.....	.....….....