SYLLABUS

1. Data about the program of study

1.1 Institution	Technical University of Cluj-Napoca
1.2 Faculty	Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master of Science
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time
1.8 Subject code	12.

2. Data about the subject

2.1 Subject name				***Computing System and Network Security Configurations***	
2.2 Course responsible / lecturer				Assoc.prof.dr.eng. Cebuc Emil - emil.cebuc@cs.utcluj.ro	
2.3 Teachers in charge of seminars				Assoc.prof.dr.eng. Iancu Bogdan - bogdan.iancu@cs.utcluj.ro	
2.4 Year of study	II	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DA
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	4	of which	Course	2	Seminar	-	Laboratory	2	Project	-
3.2 Total hours in the curriculum	56	of which	Course	28	Seminar	-	Laboratory	28	Project	-
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										25
(b) Supplementary study in the library, online and in the field										20
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										22
(d) Tutoring										0
(e) Exams and tests										2
(f) Other activities										0

3.4 Total hours of individual study (sum (3.7(a)...3.7(f)))	69
3.5 Total hours per semester (3.4+3.8)	125
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	Computer Networks, Computer Architecture
4.2 Competence	Computer Networks, Computer Architecture

5. Requirements (where appropriate)

5.1 For the course	Blackboard, projector, computers, specific software
5.2 For the applications	Classroom, PC with internet access, Computer networks equipment and software (simulators, emulators, network analysis tools, development boards, VMs). Laboratory and project attendance is mandatory

6. Specific competences

6.1 Professional competences	**C1. Identify and understand the security issues specific to the different contexts of computing system usage. Appropriately apply the basic elements of security management and methods of evaluation and management of information security risks.** • **C1.1.** Knowledge of advanced theoretical and practical terminology, concepts, and principles specific to cybersecurity field. Knowledge of concepts about cybersecurity risk evaluation, and management. • **C1.2.** Understanding cybersecurity risks specific to new situations and their relationship with previously experienced situations and risks. Be able to predict possible threat scenarios when using cybersecurity solutions in new fields or situations. • **C1.3.** Capability to identify and model new types of cybersecurity risks affecting end users, computing systems, and software applications, and identify and evaluate possible solutions against such risks. **C4. Design and develop highly secure software, security solutions and tools.** • **C4.1.** Knowledge of basic concepts and principles of secure software development and evaluation. Knowledge of common types of security software and tools. Knowledge of different operating system architectures, hardware and software infrastructures and frameworks needed to develop effective security solutions. • **C4.2.** Be able to identify new situations and scenarios when it is needed to develop a new cybersecurity solution or use an existing one. Be able to analyse proposed cybersecurity solutions and compare them with existing ones. • **C4.3.** Capability to develop complex secure software, complying with recommended good practices of built-in security and secure coding. Capability to develop software tools used for cybersecurity pen testing and assessment. • **C4.5.** Capability to develop software modules and tools that could provide a high degree of cybersecurity. Capability to propose new methods to assess the cybersecurity of computing systems and devices and ways to improve it. **C5. Develop rigorous and efficient security solutions to complex real-life problems and situations. Be able to use security mathematical tools and models, engineering approaches and technologies specific and appropriate for the information and computing system security field.** • **C5.1.** Knowledge of complex relationship between cybersecurity and real-life aspects. Knowledge of mathematical theory some cybersecurity mechanisms and solutions are based on. • **C5.4.** Capability to identify and assess limitations of existing cybersecurity solutions and tools used in real-life situations, their residual cybersecurity risks, and their criticality. Capability to identify and research new cybersecurity fields and methods that could be used to reduce the limitations of existing cybersecurity solutions.
6.2 Cross competences	N/A

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

7.1 General objective	After this course, the students will be familiar with Computer Network security concepts and will be able to build secure networks. They will also be able to configure networks services like DHCP, DNS, etc. with security issues in mind.
7.2 Specific objectives	1. Understanding the aspects of configuring VLANs and VPNs, technologies widely used in modern typical networks 2. Understanding of the elements of network activity monitoring and auditing technologies 3. Understanding the most important security aspects in the field of system and network administration 4. ….

	5. ….

8. Contents

8.1. Lecture (syllabus)	Hours	Teaching methods	Notes
Network Fundamentals Review: Network Topologies and Devices Overview	2	Presentations using slides and the blackboard, discussions, individual assignments consisting in reading and presenting research papers	
Network Fundamentals Review: IP Networking and Protocol Stack Overview	2		
Network gear security (Router and switch, console, telnet, SSH, local usernames & passwords, AAA, Port security)	2		
VLAN implementation, security issues	2		
Virtual Private Networks (VPN) Security issues	2		
Network traffic auditing, monitoring and logging.	2		
Intruder Detection and Prevention Systems IDS/IPS	2		
Layer 2 Security Threats	2		
NAT and firewall	2		
Network monitoring	2		
High Availability and Redundancy	2		
Incident handling and reporting	2		
Network security standards and policies	2		
Concepts Revision	2		

Bibliography:

Bibliography

1. Wendell Odom, David Hucaby, Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd Edition, Cisco Press, 2024.
2. Matt Oswalt, Christian Adell, Scott Lowe, Jason Edelman, Network Programmability and Automation: Skills for the Next-Generation Network Engineer 2nd Edition, O'Reilly Media, 2018 and 2023.
3. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition, Morgan Kaufmann, 2021.
4. Perry Lea, IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security, 2nd Edition, Packt Publishing, 2020.
5. Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Pearson Education, 2020.
6. The Practice of System and Network Administration (Limonceli, Thomas – 2007 – Addison-Wesley) (2nd ed). UNIX and Linux System Administration Handbook (Nemeth, Evi – 2010 – Prentice Hall) (4th ed).

8.2 Applications - Seminars / Laboratory / Project	Hours	Teaching methods	Notes
Review of basic computer networking knowledge: IPv4, IPv6, DHCP, NAT/PAT, Wireshark.	2	Short presentations, work guides, live demos, discussions, problems solving	
Security, authentication, and monitoring: Telnet, SSH, local usernames & passwords, AAA	2		
Security, authentication, and monitoring: AAA, Port Security, 802.1X	2		
Virtual LAN implementation and VLAN security	2		
Implementation of firewall and IPS functions at network equipment level: access control lists (IPv4, IPv6 ACLs)	2		
Implementation of firewall and IPS functions at network equipment level: VPNs	2		
Security, authentication, and monitoring: SNMP, Syslog, NetFlow	2		
Security, authentication, and monitoring: Network inspection tools	2		
L2 security, spoofing and phishing	2		
High Availability and Redundancy	2		

Firewall rules and configurations	2		
NetFlow and interpreting server logs	2		
Security in wireless LAN and mobile networks	2		
Laboratory test	2		

Bibliography:

1. Wendell Odom, David Hucaby, Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd Edition, Cisco Press, 2024.
2. Matt Oswalt, Christian Adell, Scott Lowe, Jason Edelman, Network Programmability and Automation: Skills for the Next-Generation Network Engineer 2nd Edition, O'Reilly Media, 2018 and 2023.
3. David D. Coleman, David A. Westcott, CWNA Certified Wireless Network Administrator Study Guide, Sybex, 2021.
4. Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Pearson Education, 2020.
5. Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackim UNIX and Linux System Administration Handbook, 5th Edition, Addison-Wesley Professional, 2017.

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

It is done through discussions with representants with the most significant employers, especially those active in the cybersecurity field.

Multiple master programs abroad offer network security optional courses:

- Security Architectures and Network Defence, Master in Cyber Security and Management, The University of Warwick, IK, http://www2.warwick.ac.uk/fac/sci/wmg/education/wmgmasters/structure/modules/sand
- *Securitatea rețelelor de calculatoare*, Master de Securitatea tehnologiei informației, Academia Tehnică Militară, București, http://mta.ro/masterat/masterinfosec/curricula2014.html
- *Networking and Systems Requirement*, Master of Science in Information Security, Carnegie Mellon University, SUA, http://www.ini.cmu.edu/degrees/msis/courses.html
- *Network Security* și *Secure Operating Systems*, Master of Engineering in Cybersecurity, Cybersecurity Center,
- University of Mayland, http://www.cyber.umd.edu/education/meng-cybersecurity

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Problem-solving skills specific to the network security field. Attendance and active participation during lectures.	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of different subjects / paper in the course's field during semester time.	70%
Laboratory	Problem-solving skills specific to thenetwork security field. Attendance and active participation during labs.	Evaluate lab activity. Evaluate lab assignments (homework). Evaluate solutions of problems given in a final lab exam.	30%

Minimum standard of performance

***Lecture*.** Attending **minimum 50%** of lecture classes, to be allowed to take the final examination. Students must be able to define and describe fundamental aspects regarding networking devices and their security mechanisms. Minimum final grade must be 5 for the exam to be considered passed.

***Lab*.** Attending **all lab classes** (one lab could be recovered during the semester, and one more during re-examination sessions). Students must be able to identify fundamental network vulnerabilities. This kind of assessment could happen in relation to assignments given during semester or subjects given during the final lab evaluation. Minimum lab grade

must be 5 for being allowed at final exam.

Date of filling in: 26.02.2025	Responsible	Title First name Last name	Signature
	Course	Assoc.prof.dr.eng. Emil CEBUC	
	Applications	Assoc.prof.dr.eng. Bogdan IANCU	

Date of approval in the Computer Science Department	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the faculty of Automation and Computer Science	Dean, Prof.dr.eng. Vlad Mureșan