SYLLABUS

1. Data about the program of study

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

2. Data about the subject

2.1 Subject name	***Computing System and Network Security Configurations***			Subject code	**12**
2.2 Course responsible / lecturer	Assoc. prof. dr. eng. Cebuc Emil - emil.cebuc@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	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: DF – fundamental, DS – speciality, DC – complementary				DF
	Optionality: DOB – mandatory, DOP – optional (alternative), DFA – optional (free choice)				DOB

3. Estimated total time

3.1 Number of hours per week	4	of which:	Course	2	Seminars	-	Laboratory	2	Project	-
3.2 Number of hours per semester	56	of which:	Course	28	Seminars	-	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										-
(e) Exams and tests										2
(f) Other activities:										-

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	69
3.5 Total hours per semester (3.2+3.4)	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, PC MS Teams Platform, Moodle Platform
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 competence

6.1 Professional competences	Gradutes: • implement ICT risk management • develop information security strategy • perform ICT security testing • manage disaster recovery plans • execute ICT audits • develop contingency plans for emergencies • manage system security • implement ICT recovery system • manage IT security compliances • identify ICT security risks • define security policies • perform risk analysis • educate on data confidentiality • provide ICT consulting advice • perform data analysis • establish an ICT security prevention plan • implement ICT security policies • ensure compliance with legal requirements • ensure information privacy • monitor developments in field of expertise • keep up with the latest information systems solutions
6.2 Cross competences	The graduate's competences: • develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded • coordinate engineering teams

7. Expected Learning Outcomes

Knowledge	The student has knowledge of: • ICT security standards • Internet of Things (IoT) • computer programming • cyber attack counter-measures • digital systems • embedded systems • information security strategy • security engineering • software anomalies • ICT encryption • ICT safety • cloud technologies • ethical hacking principles • organisational resilience • ICT network security risks • internet governance • network standards • operating systems • quality assurance methodologies • system backup best practices • ICT infrastructure • ICT security legislation • cloud monitoring and reporting • computer forensics

	• cyber security • information confidentiality • telecom regulations • web application security threats • GDPR • attack vectors • building systems monitoring technology • incidents and accidents recording • operational tactics for emergency responses • risk management • security threats • business intelligence • copyright legislation • defence standard procedures • leadership principles • project management • ICT performance analysis methods • assessment of risks and threats • internal risk management policy • open source model • outsourcing model • audit techniques • decision support systems • domain name service (DNS) • hybrid model • investment analysis • legal requirements of ICT products • systems development life cycle • tools for ICT test automation
Skills	The student is able to: • analyse ICT systems • create flowchart diagrams • define security policies • define technical requirements • develop ICT device drivers • develop software prototypes • identify ICT security risks • identify ICT system weaknesses • interpret technical texts • keep up with the latest information systems solutions • manage IT security compliances • monitor system performance • perform ICT security testing • perform risk analysis • provide ICT consulting advice • report test findings • use software libraries • utilise computer-aided software engineering (CASE) tools • debug software • develop creative ideas • integrate system components • perform project management • apply company policies • attend to ICT systems quality • ensure proper document management • maintain ICT identity management

	• maintain database security • manage ICT data architecture • perform ICT troubleshooting • solve ICT system problems • address problems critically • assess ICT knowledge • build business relationships • execute ICT audits • implement ICT security policies • implement a firewall • implement a virtual private network (VPN) • lead disaster recovery exercises • manage ICT virtualisation environments • manage cloud data and storage • manage databases • manage keys for data protection • perform backups • protect personal data and privacy • remove computer viruses or malware • respond to incidents in cloud environments • store digital data and systems • train employees • use scripting languages for programming • collect cyber defence data • communicate with stakeholders • cope with stress • create incident reports • engage with stakeholders • handle cybersecurity incidents • protect ICT devices • consult with business clients • create project specifications • define quality standards • develop an information security strategy • ensure information security • give live presentations • implement spam protection • manage ICT change request processes • manage changes in ICT systems • manage digital identity • optimise the choice of ICT solutions • perform scientific research • provide information • provide user documentation • track key performance indicators (KPIs) • troubleshoot • advise on security risk management • ensure adherence to organisational ICT standards • establish an ICT security prevention plan • establish an Information Security Management System (ISMS) • manage systems • define technology strategy • design for organisational complexity • develop with cloud services • manage disaster recovery plans • use an ICT ticketing system

	• use an application-specific interface • use backup and recovery tools
Responsibilities and autonomy	The student has the ability to work independently in order to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded • coordinate engineering teams

8. Discipline objective (as results from the *key competences gained*)

8.1 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.
8.2 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

9. Contents

9.1 Lectures	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

- Wendell Odom, David Hucaby, Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd Edition, Cisco Press, 2024.
- 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.
- Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition, Morgan Kaufmann, 2021.
- 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.
- Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Pearson Education, 2020.

- 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).

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Review of basic computer networking knowledge: IPv4, IPv6, DHCP, NAT/PAT, Wireshark.	2	Oral presentation using slides, discussions, (Q&A). Practical exercises Presentation of possible solutions Self-testing programme.	
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

- Wendell Odom, David Hucaby, Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd Edition, Cisco Press, 2024.
- 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.
- David D. Coleman, David A. Westcott, CWNA Certified Wireless Network Administrator Study Guide, Sybex, 2021.
- Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Pearson Education, 2020.
- Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackim UNIX and Linux System Administration Handbook, 5th Edition, Addison-Wesley Professional, 2017.

10. 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

11. 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	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of	50%

	during lectures	different subjects / paper in the course's field during semester time. Intermediary and summative.	
Laboratory	Problem-solving skills specific to the network 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. Intermediary and summative.	50%

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: 29.04.2026	**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 department	Head of department, Prof. dr. eng. Rodica Potolea
Date of approval in the Faculty Council	Dean, Prof. dr. eng. Vlad Mureșan