

Cyber-physical Systems Institute			Semester 6. of the curriculum 2025-26-2			
Name of the subject:	Code of the subject:	Credits:	Weekly hours:			
				lec	sem	lab
Security of Computer Networks and Clouds	NBXS F1EBNF		full-time	2	0	2
Responsible person for the subject: Vörösné Dr. Bánáti-Baumann Anna			Classification: Senior lecturer			
Subject lecturer(s): Balázsné Dr. Kail Eszter, Farkas Attila						
Prerequisites:	NKXHT1EBNF	Network Technologies				
Way of the assessment:	Exam					
Course description						
Goal:	The aim of the course Computer Networks and Cloud Security is to provide students with in-depth knowledge of the security challenges and solutions related to both traditional network infrastructures and modern cloud-based environments. Emphasizing both theoretical foundations and hands-on practice, the course prepares students to design, operate, and manage secure systems. Key areas include threat prevention, secure architecture, attack detection and response, and the application of industry security standards and best practices.					
Course description:	This course provides an in-depth overview of modern network and cloud security practices, with a focus on applied knowledge and real-world relevance. Students begin by exploring fundamental principles of network security and the hardening of network devices, including authentication, authorization, and accounting (AAA). Key threats at Layer 2 are discussed alongside their mitigation strategies. The course covers both traditional access control lists (ACL) and modern next-generation firewalls (NGFW), as well as intrusion detection and prevention systems (IDS/IPS). In the cloud segment, students gain hands-on experience with OpenStack, focusing on identity management, virtual machine isolation, and network protection. The course also addresses VPN technologies and the challenges of inspecting encrypted traffic. Students learn to perform vulnerability assessments, use threat intelligence sources, and build awareness of logging practices, monitoring strategies, and Security Operations Center (SOC) functions.					

Lecture schedule	
Education week	Topic
1.	Introduction to Security of Computer networks
2.	Network device harden and AAA
3.	Layer 2 attacks and their countermeasures
4.	Firewalls I. - ACL
5.	Firewalls II. - NGFW
6.	OpenStack basics and user management
7.	OpenStack virtual machine and network security
8.	Holiday
9.	IDS/IPS
10.	VPN – analyses of encrypted traffic
11.	Vulnerability scanning, vulnerability intelligence sharing and
12.	Logging and monitoring, SOC
13.	Lab exam

14.	Lab exam retake												
Mid-term requirements													
Conditions for obtaining a mid-term grade/signature	Participation at the lessons is mandatory. Students who missed more than 30% of lessons should take a signature retake exam. A successful test is mandatory to acquire grade.												
Assessment schedule													
Education week	Topic												
13.	Lab exam												
14.	Lab exam retake												
Method used to calculate the <i>mid-term grade</i> (to be filled out only for subjects with mid-term grades)													
Test result needs to exceed 51%.													
Type of the replacement													
Type of the replacement of written test/mid-term grade/signature	In the case if the mid-term test does not reach 50%, the student can replace the test in the form of re-take test in the 14th week. Replacement of the mid-term mark: once in the first 10 working days of the examination period.												
Type of the exam (to be filled out only for subjects with exams)													
The exam consists of a lab exam and an oral exam													
Calculation of the exam mark (to be filled only for subjects with exams)													
The final grade will be calculated as the average of the results of the lab exam and the oral exam, but both must reach at least 51%.													
Final grade calculation methods:													
The final grade will be calculated using the following scale:													
	<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Achieved result</th> <th>Grade</th> </tr> </thead> <tbody> <tr> <td>87% - 100%</td> <td>excellent (5)</td> </tr> <tr> <td>75%- 86%</td> <td>good (4)</td> </tr> <tr> <td>64% -74%</td> <td>satisfactory (3)</td> </tr> <tr> <td>51% - 63%</td> <td>pass (2)</td> </tr> <tr> <td>0 - 50 %</td> <td>failed (1)</td> </tr> </tbody> </table>	Achieved result	Grade	87% - 100%	excellent (5)	75%- 86%	good (4)	64% -74%	satisfactory (3)	51% - 63%	pass (2)	0 - 50 %	failed (1)
Achieved result	Grade												
87% - 100%	excellent (5)												
75%- 86%	good (4)												
64% -74%	satisfactory (3)												
51% - 63%	pass (2)												
0 - 50 %	failed (1)												
References													
Obligatory:	Lecture notes, Cisco Network Academy course material												
Recommended:	<ul style="list-style-type: none"> – Fundamentals of Network Security Companion Guide (Cisco Networking Academy Program) Cisco Systems, Cisco Networking Academy Program, ISBN: 1587131226 – Fundamentals of Network Security Lab Companion and Workbook (Cisco Networking Academy Program) Cisco Systems, Inc., Cisco Networking Academy Program. ISBN: 1587131234 – Matt Dorn, Preparing for the Certified OpenStack Administrator Exam, Packt Publishing, ISBN: 1787288412 												
Other references:													