S Y L L A B U S

<table>
<tr><td rowspan="8">General information</td><td>Title and code of subject, number of credits</td><td colspan="3">CMS 413 - Network Security</td></tr>
<tr><td>Department</td><td colspan="3">Computer Science & Engineering</td></tr>
<tr><td>Program</td><td colspan="3">Bachelor. - 6 credits</td></tr>
<tr><td>Academic semester</td><td colspan="3">Spring, 2023</td></tr>
<tr><td>Lecturer</td><td colspan="3">Behnam Kiani</td></tr>
<tr><td>E-mail:</td><td colspan="3">bkiani@khazar.org</td></tr>
<tr><td>Phone number:</td><td colspan="3"></td></tr>
<tr><td>Lecture room/Schedule</td><td colspan="3">11 Mehseti Street, AZ1096 Baku, Azerbaijan (Neftchilar campus), Class room: N406</td></tr>
<tr><td></td><td>Consultations</td><td colspan="3"></td></tr>
<tr><td>Course language</td><td colspan="4">English</td></tr>
<tr><td>Type of the subject</td><td colspan="4">Major</td></tr>
<tr><td>Textbooks and additional materials</td><td colspan="4">1. C omputer Security Principles and Practice Fourth Edition Global Edition William Stallings Lawrie Brown-2018
2. CompTIA® Security+ Guide to Network Security Fundamentals, Seventh Edition Mark Ciampa, © 2022Cengage Learning, Inc.</td></tr>
<tr><td rowspan="2">Teaching methods</td><td colspan="3">Lecture</td><td>15</td></tr>
<tr><td colspan="3">Group discussions at seminars</td><td>15</td></tr>
<tr><td rowspan="5">Assessment</td><td colspan="2">Components</td><td>Date/ Deadline</td><td>Percent (%)</td></tr>
<tr><td colspan="2">Project</td><td></td><td>20%</td></tr>
<tr><td colspan="2">Attendance</td><td></td><td>5%</td></tr>
<tr><td colspan="2">Midterm Exam</td><td>Midterm Exam</td><td>35%</td></tr>
<tr><td colspan="2">Final Exam</td><td>Final Exam</td><td>40%</td></tr>
<tr><td>Course description</td><td colspan="4">This course introduces the underlying concepts and principles of advanced computer networks. It presents the different components of a network and how these components fit together. This course discusses about internet network architecture, the various advanced protocols and technologies, The course emphasizes the design and implementation of network software that transforms raw hardware into a richly functional communication system. Real networks are used as examples to reinforce the concepts and demonstrate various protocols.</td></tr>
<tr><td>Course objectives</td><td colspan="4">Introduction to analysis and design of ISP networks through understanding the network layered architecture and the protocol stack and by conducting hands-on programming and lab activities, how to use internet through end-to-end technology.</td></tr>
<tr><td>Learning outcomes</td><td colspan="4">By the end of the Course students should be able:
▪ Be familiar with the different Network Models.
▪ Understand different network technologies.
▪ Understand the effects of using different networking topologies.
▪ Be updated with different advanced network technologies that can be used to connect different networks.
▪ Be familiar with various hardware and software that can help protect the network.
▪ Know the advantage of using a network management system.
▪ Practical skills to configure and manage network devices</td></tr>
<tr><td>Rules (Educational policy and behavior)</td><td colspan="4">▪ Preparation for class
The structure of this course makes your individual study and preparation outside the class extremely important. The lecture material will focus on the major points introduced in the text. Reading the assigned chapters and having some familiarity with them before class will greatly assist your understanding of the lecture. After the lecture, you should study your notes and work relevant problems and cases from the end of the chapter and sample exam questions.
Throughout the semester we will also have a large number of review sessions. These</td></tr>
</table>

	review sessions will take place during the regularly scheduled class periods. ▪ **Withdrawal (pass/fail)** This course strictly follows grading policy of the School of Economics and Management. Thus, a student is normally expected to achieve a mark of at least 60% to pass. In case of failure, he/she will be required to repeat the course the following term or year. ▪ **Cheating/plagiarism** Cheating or other plagiarism during the Quizzes, Mid-term and Final Examinations will lead to paper cancellation. In this case, the student will automatically get zero (0), without any considerations. ▪ **Professional behavior guidelines** The students shall behave in the way to create favorable academic and professional environment during the class hours. Unauthorized discussions and unethical behavior are strictly prohibited.

This program reflects the comprehensive information about the subject and information about any changes will be provided in advance.

Week	Dates (planned)	Subject topics	Textbook/ Assignments
1	*Week 1*	**Chapter 1 Overview** 1.1 Computer Security Concepts 1.2 Threats, Attacks, and Assets 1.3 Security Functional Requirements 1.4 Fundamental Security Design Principles 1.5 Attack Surfaces and Attack Trees 1.6 Computer Security Strategy **1.7 Standards**	**Chapter 1 Overview**
2	*Week 2*	**Chapter 2 Cryptographic Tools** 2.1 Confidentiality with Symmetric Encryption 2.2 Message Authentication and Hash Functions	**Chapter 2 Cryptographic Tools**
3	*Week 3*	2.3 Public-Key Encryption 2.4 Digital Signatures and Key Management 2.5 Random and Pseudorandom Numbers **2.6 Practical Application: Encryption of Stored Data**	**Chapter 2 Cryptographic Tools**
4	*Week 4*	**Chapter 3 User Authentication** **3.1** Digital User Authentication Principles **3.2** Password-Based Authentication **3.3** Token-Based Authentication	**Chapter 3 User Authentication**
5	*Week 5*	**3.4** Biometric Authentication **3.5** Remote User Authentication **3.6** Security Issues for User Authentication **3.7 Practical Application: An Iris Biometric System**	**Chapter 3 User Authentication**
6	*Week 6*	**Chapter 4 Access Control** **4.1** Access Control Principles **4.2** Subjects, Objects, and Access Rights **4.3** Discretionary Access Control **4.4** Example: UNIX File Access Control	**Chapter 4 Access Control**
7	*Week 7*	**4.5** Role-Based Access Control **4.6** Attribute-Based Access Control **4.7** Identity, Credential, and Access Management **4.8 Trust Frameworks 158**	**Chapter 4 Access Control**

8	*Week 8*	**Midterm Exam**	
9	*Week 9*	**Chapter 5 Database and Data Center Security** **5.1** The Need for Database Security **5.2** Database Management Systems **5.3** Relational Databases	**Chapter 5 Database and Data Center Security**
10	*Week 10*	**Chapter 6 Malicious Software** **6.1** Types of Malicious Software (Malware) **6.2** Advanced Persistent Threat **6.3** Propagation—Infected Content—Viruses **6.4** Propagation—Vulnerability Exploit—Worms **6.5** Propagation—Social Engineering—Spam E-mail, Trojans	**Chapter 6 Malicious Software**
11	*Week 11*	**6.6** Payload—System Corruption **6.7** Payload—Attack Agent—Zombie, Bots **6.8** Payload—Information Theft—Keyloggers, Phishing, Spyware **6.9** Payload—Stealthing—Backdoors, Rootkits	**Chapter 6 Malicious Software**
12	*Week 12*	**Chapter 7 Denial-of-Service Attacks** **7.1** Denial-of-Service Attacks **7.2** Flooding Attacks **7.3** Distributed Denial-of-Service Attacks	**Chapter 7 Denial-of-Service Attacks**
13	*Week 13*	**7.4** Application-Based Bandwidth Attacks **7.5** Reflector and Amplifier Attacks **7.6** Defenses Against Denial-of-Service Attacks **7.7** Responding to a Denial-of-Service Attack	**Chapter 7 Denial-of-Service Attacks**
14	*Week 14*	**Chapter 8 Firewalls and Intrusion Prevention Systems** **8.1** The Need for Firewalls **8.2** Firewall Characteristics and Access Policy **8.3** Types of Firewalls **8.4** Firewall Basing **8.5** Firewall Location and Configurations **8.6** Intrusion Prevention Systems	**Chapter 8 Firewalls and Intrusion Prevention Systems**
		Final Exam	