## Course Name : Basics of Cyber Security

| Course Code | Course Type | Regular Semester | Lecture (hours/week) | Seminar (hours/week) | Lab. (hours/week) | Credits | ECTS |
|---|---|---|---|---|---|---|---|
| CMP 505 | B | Fall | 3.00 | 1.00 | 0.00 | 3.50 | 6.00 |

| | |
|---|---|
| **Lecturer** | Sadije Bushati, Prof. Dr |
| **Assistant** | Rexhion Qafa, Msc |
| **Course language** | Albanian |
| **Course level** | Master |
| **Description** | The course “Basics of Cyber Security” introduces the fundamental concepts of protecting computer systems and networks against security threats. Students will explore security mechanisms such as encryption, authentication, access control, intrusion detection, and risk management. |
| **Objectives** | To understand fundamental concepts in cyber security. To learn encryption algorithms and authentication techniques. To assess risks and threats in computer systems. To design security policies for networks and organizations. |
| **Core Concepts** | Security principles: confidentiality, integrity, availability Symmetric and asymmetric cryptography Authentication, authorization, and access control Network security and firewalls Malware, phishing, and social engineering Risk management and incident response |

## Course Outline

| Week | Topic |
|---|---|
| **1** | Introduction to Cyber Security |
| **2** | Basic Security Principles (CIA Triad) |
| **3** | Symmetric Cryptography (AES, DES) |
| **4** | Asymmetric Cryptography (RSA, ECC) |
| **5** | Hashing and Integrity Checking |
| **6** | Authentication and Security Protocols |
| **7** | Access Control and IAM Systems |
| **8** | Midterm Exam |
| **9** | Network Security and Firewall Technologies |
| **10** | Intrusion Detection Systems (IDS/IPS) |
| **11** | Malware and Protection Techniques |
| **12** | Social Engineering and Cyber Fraud |
| **13** | Risk Management and Security Policies |
| **14** | Cloud & Mobile Security |
| **15** | Project Presentations and Case Studies |
| **16** | Final Exam |

| | |
|---|---|
| **Prerequisites** | The student must attend the course at a minimum rate of 75%. |
| **Literature** | • William Stallings – Network Security Essentials: Applications and Standards, 6th Edition, Pearson, 2023. |
| **References** | • Charles P. Pfleeger & Shari Lawrence Pfleeger – Security in Computing, 5th Edition, Pearson, 2015.<br>• Mark Stamp – Information Security: Principles and Practice, Wiley, 2019.<br>• Bruce Schneier – Applied Cryptography, Wiley, 2015. |

## Course Outcome

| | |
|---|---|
| **1** | Students will understand the fundamentals of data and network protection. |
| **2** | They will apply security mechanisms such as encryption and access control. |
| **3** | They will analyze threats and propose countermeasures. |
| **4** | They will develop the ability to manage incidents and create security policies. |

## Course Evaluation

| In-term Studies | Quantity | Percentage |
|---|---|---|
| Midterms | 1 | 40 |
| Quizzes | 0 | 0 |
| Projects | 0 | 0 |
| Term Projects | 0 | 0 |
| Laboratory | 0 | 0 |
| Class Participation | 0 | 0 |
| **Total in-term evaluation percent** | | **40** |
| **Final exam percent** | | **60** |
| **Total** | | **100** |

## ECTS Workload (Based on Student Workload)

| Activities | Quantity | Duration (hours) | Total (hours) |
|---|---|---|---|
| Course duration (Including the exam week: 16x Total hours of the course) | 16 | 4 | 64 |
| Study hours outside the classroom (Preparation, Practice, etc.) | 14 | 5 | 70 |
| Duties | 0 | 0 | 0 |
| Midterms | 1 | 6 | 6 |
| Final Exam | 1 | 8 | 8 |
| Other | 0 | 0 | 0 |
| **Total Work Load** | | | **148** |
| **Total Work Load / 25 (hours)** | | | **5.92** |
| **ECTS** | | | **6.00** |