B. Tech (Program) Honors/Minor* in Cyber Security and Forensics
T. Y. B. Tech. Computer Engineering
Pattern 2022 Semester: VI
COM223022: Cyber Security Lab-I

Teaching Scheme:	Credit Scheme:	Examination Scheme:
Practical: 04 hrs/week	02	Termwork:50 Marks Oral Exam :50 Marks

Prerequisite Courses: - COM223009 Data Communication and Networking

Course Objectives:
- To Understanding Cyber Space and Information Systems
- To Identifying and Analyzing Cyber Threats
- To Implementing Security Technologies
- To Evaluating and Developing Security Solutions

Course Outcomes: On completion of the course, students will be able to–

	Course Outcomes	Bloom's Level
CO1	Describe Key Concepts and Components of Cyber Space and Information Systems	3-Undertand
CO2	Analyze and Classify Different Types of Cyber Attacks and Malware	4-Analyze
CO3	Implement and Demonstrate Intrusion Detection Systems and Biometric Authentication Methods	3-Apply
CO4	Implement Security Models and Develop Security Solutions for Web Applications	3-Apply

List of Laboratory Experiments / Assignments

Sr. No.	Laboratory Experiments / Assignments	CO Mapped
1	**Assignment: Exploring Cyber Space Components** • **Objective:** Understand the basic components and dynamics of cyber space. • **Tasks:** ○ Identify and list the key components of cyber space. ○ Describe the role and function of each component. ○ Create a diagram illustrating the interaction between these components. • **Tools Required:** Diagramming software (e.g., Microsoft Visio, Lucidchart).	CO1
2	• **Objective:** Understand the structure and role of information systems in cyber space. • **Tasks:** • Select an organization and analyze its information system. • Identify the main components and their functions.	CO1

	• Explain how the information system supports the organization's operations. **Tools Required:** Research materials, word processing software.	
3	**Assignment: Cyber Attack Case Study** • **Objective:** Analyze real-world cyber attacks and understand their impact. • **Tasks:** • Research a recent cyber attack and document the details (method, impact, response). • Identify the type of attack and classify it based on the classification learned. • Suggest possible mitigation strategies to prevent similar attacks. • **Tools Required:** Internet access, word processing software.	CO2
4	• **Objective:** Identify and analyze different types of malware. • **Tasks:** • Obtain malware samples (e.g., from a controlled lab environment or online databases). • Use tools like VirusTotal to analyze the malware behavior. • Document the characteristics and potential mitigation techniques for each type of malware. **Tools Required:** Virtual machine, VirusTotal, anti-malware tools.	CO2
5	**Assignment: Configuring Intrusion Detection Systems** • **Objective:** Gain hands-on experience with intrusion detection systems. • **Tasks:** • Install and configure Snort (or any IDS) on a virtual machine. • Create and test custom rules to detect specific types of network traffic. • Document the process and results, including any alerts generated. • **Tools Required:** Virtual machine, Snort, network traffic generator.	CO3
6	**Assignment: Implementing Biometric Authentication** • **Objective:** Understand and implement biometric authentication methods. • **Tasks:** • Develop a simple fingerprint or facial recognition authentication system using OpenCV. • Test the system with multiple users to evaluate its accuracy and reliability. • Document the implementation steps and results. • **Tools Required:** OpenCV, Python, webcam or fingerprint sensor.	CO4
7	**Assignment: Evaluating Security Models** • **Objective:** Evaluate the effectiveness of various security models and mechanisms.	CO4

	• **Tasks:** • Select two different security models (e.g., Bell-LaPadula, Biba). • Compare and contrast their principles and applications. • Evaluate their effectiveness in a given scenario (e.g., securing a financial system). • **Tools Required:** Research materials, word processing software.	
8	**Assignment: Securing a Web Application** • **Objective:** Identify and mitigate security vulnerabilities in a web application. • **Tasks:** • Use OWASP ZAP to perform a security audit on a given web application. • Identify and document vulnerabilities such as SQL injection, XSS, and CSRF. • Implement mitigation strategies and re-test the application. • **Tools Required:** OWASP ZAP, web application (e.g., DVWA).	CO4
9	**Assignment: Digital Forensics Investigation** • **Objective:** Conduct a digital forensic investigation on a compromised system. • **Tasks:** • Use FTK Imager to create a disk image of a compromised system. • Analyze the disk image for evidence of malicious activity. • Document the findings and suggest steps for remediation. • **Tools Required:** FTK Imager, virtual machine.	CO1-CO4
10	**Assignment: Legal Aspects of Cyber Security** • **Objective:** Understand the legal framework governing cyber security. • **Tasks:** • Research the Information Technology Act 2000 and its amendments. • Prepare a report on key provisions relevant to cyber crimes and digital forensics. • Discuss the legal implications of a recent cyber crime case.	CO1-CO4

	- **Tools Required:** Research materials, word processing software.	

Guidelines for Laboratory Conduction

Use of coding standards and Hungarian notation, proper indentation and comments.
Use of open-source software is to be encouraged.
Operating System recommended: - Linux or its derivative
Programming tools recommended: - Python

Guidelines for Student's Lab Journal

The laboratory assignments are to be submitted by students in the form of a journal. Journal consists of Certificate, table of contents, and handwritten write-up of each assignment (Title, problem statement, theory concepts in brief, algorithm, flowchart, test cases and conclusions). Program codes with sample outputs shall be submitted in soft form

Guidelines for Termwork Assessment

Continuous assessment of laboratory work shall be based on overall performance of a student. Assessment of each laboratory assignment shall be based on rubrics that include R1- timely completion (10), R2- understanding of assignment (10) and R3- presentation/clarity of journal writing (10) (Coding standard, Indentation, Hungarian notation, input validation etc)

Strength of CO-PO PSO Mapping

	PO												PSO	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	2	-	-	3	-	-	-	-	-	-	-	-	-
CO2	3	3	-	-	3	-	-	-	-	-	-	-	-	-
CO3	3	3	-	-	3	-	-	-	-	-	-	-	-	-
CO4	3	3	-	-	3	-	-	-	-	-	-	-	-	-
Average	3	2.75	-	-	3	-	-	-	-	-	-	-	-	-