

25MCST303	INTRODUCTION TO CYBER SECURITY	Category	L	T	P	R	Credit	Year of Introduction
		VAC	4	0	0	0	4	2025

Preamble: Cyber security has become a critical domain to safeguard information, systems, and networks from unauthorized access, attacks, and data loss. Organizations across all sectors require skilled professionals who can identify vulnerabilities, implement security measures, and respond effectively to cyber incidents. This course provides a comprehensive understanding of cyber security fundamentals, threat analysis, network and system security mechanisms, and legal and ethical aspects of cyber space.

Prerequisite: Nil

Course Outcomes: After the completion of the course, the student will be able to:

CO	Course Outcomes	Knowledge Level
CO1	Explain the fundamentals of cyber security, information security concepts, and various types of cyber threats and attacks.	K2 Understand
CO2	Apply security tools and techniques to perform vulnerability assessments, identify potential attack surfaces, and recommend suitable mitigation strategies	K3 Apply
CO3	Describe the fundamental security mechanisms used in network, web, and operating systems to protect data from unauthorized access	K3 Understand
CO4	Explain cyber laws, ethical hacking principles, and incident response procedures for handling security breaches.	K2 Understand

Mapping of course outcomes with program outcomes and program specific outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	1	-	-	-	-	-	-	-	-	1	3	1
CO2	2	3	-	2	-	-	-	-	-	-	1	3	2
CO3	2	2	2	1	-	1	-	-	-	-	1	3	3
CO4	1	1	-	-	-	2	3	-	-	-	1	3	1
Avg	1.75	1.75	2	1.5	-	1.5	3	-	-	-	1	3	1.75

Mapping of course outcomes with Knowledge and Attitude Profile (WK)

	WK1	WK2	WK3	WK4	WK5	WK6	WK7	WK8	WK9
CO1	*	*	*	*				*	
CO2	*	*	*	*				*	
CO3	*	*	*	*	*		*	*	
CO4	*	*	*	*	*		*	*	*

Wks Mapped with the course

WK1	WK2	WK3	WK4	WK5	WK6	WK7	WK8	WK9
*	*	*	*	*		*	*	*

Mark Distribution:

Total Marks	CIE Marks	ESE Marks	ESE Duration
100	40	60	2.5 hrs

Continuous Internal Evaluation Pattern:

Attendance	: 5 marks
Continuous Assessment Test	: 20 marks
Continuous Assessment Assignment	: 15 marks

SYLLABUS

Module 1 (14 hrs)

Introduction to Cyber Security and Information Security, Types of Cyber Threats and Attacks, Hackers and Attack Vectors, Risk, Vulnerability, and Security Controls, Security Policies and Basic Security Principles

Module 2 (14 hrs)

Basics of Vulnerability Assessment and Mitigation Techniques, Social Engineering Attacks, Password Attacks and Authentication Attacks, DNS Poisoning + ARP Poisoning, Replay attack and privilege Escalation, Malware & DDoS Attacks, DoS and DDoS Attacks

Module 3 (14 hrs)

Network Security Concepts, Firewalls, IDS/IPS, VPN, Secure Communication Protocols (SSL/TLS, HTTPS, SSH), Operating System Security Mechanisms, Web Application Security (SQL Injection, XSS, CSRF), Access Control and Authentication Mechanisms

Module 4 (14 hrs)

Cyber Laws in India, Cyber Crimes and Legal Framework, Ethical Hacking Concepts and Phases, Digital Evidence and Cyber Forensics Basics, Incident Response Process, Cyber Security Best Practices and Policies

Text Books:

1. Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning. (India release 2023).
2. Stallings, W., & Brown, L. (2024). *Computer security: Principles and practice* (5th ed.). Pearson.

Reference Books:

1. Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network security*. Prentice Hall of India.
2. Nina Godbole, N., & Belapure, S. (n.d.). *Cyber security*. Wiley.
3. Maiwald, E. (2001). *Network security: A beginner's guide*. McGraw-Hill.

END SEMESTER EXAMINATION – MODEL QUESTION PAPER

Course Code	25MCST303
Course Name	INTRODUCTION TO CYBER SECURITY
Max. Marks: 60	Duration: 2.5 Hours

Part A

(Answer all questions. Each question carries 3 marks)

Qn No.	Question	Marks	CO	BL
1	Explain the difference between Cyber Security and Information Security.	3	1	L2
2	Describe the role of security controls in reducing cyber risks.	3	1	L2
3	Differentiate between a vulnerability and a threat.	3	2	L2
4	An organization identifies several unused open ports on its network devices. Apply appropriate mitigation techniques to reduce the associated security risks.	3	2	L3
5	A company network is experiencing unauthorized access attempts from external IP addresses. Apply an appropriate firewall rule to secure the server and justify your choice.	3	3	L3
6	Summarize the importance of firewalls, IDS/IPS, and VPNs in a secure network architecture.	3	3	L2
7	Describe the significance of cyber laws in regulating activities in cyberspace.	3	4	L2
8	Outline the major phases involved in ethical hacking.	3	4	L2

Part B (Answer any one full question from each Module. Each carry 9 marks)				
Module I				
Qn No.	Question	Marks	CO	BL
9	Summarize the common cyber threats faced by organizations and the security measures adopted to mitigate them.	9	1	L2
OR				
10	Describe how security controls contribute to risk management and protection of information systems.	9	1	L2
Module II				
Qn No.	Question	Marks	CO	BL
11	A company discovers that attackers have replayed previously captured authentication tokens to access restricted resources. Demonstrate how secure authentication protocols can be applied to prevent replay attacks.	9	2	L3
OR				
12	During a cyber incident, attackers perform DNS poisoning to redirect users to a fake website and then launch credential theft attacks. Apply suitable security controls to identify, contain, and mitigate the attacks.	9	2	L3
Module III				
Qn No.	Question	Marks	CO	BL
13	An organization allows employees to access its internal network remotely. To secure the communication, the administrator plans to deploy a VPN, Firewall, and SSL/TLS-based secure communication . a) Apply an appropriate firewall configuration to control incoming and outgoing traffic for remote users. (3 Marks) b) Explain how a VPN can be implemented to provide secure remote access to employees. (3 Marks) c) Demonstrate how SSL/TLS ensures confidentiality and integrity during data transmission between a client and server. (3 Marks)	9	3	L3
OR				
14	A web application used by a university stores student information in a database. During testing, security vulnerabilities related to SQL Injection, Cross-Site Scripting (XSS), and Authentication Mechanisms are identified. a) Apply suitable input validation and parameterized query techniques to prevent SQL Injection attacks. (3 Marks)	9	3	L3

	b) Demonstrate how output encoding and content filtering can be used to mitigate XSS attacks. (3 Marks) c) Apply an appropriate authentication and access control mechanism to ensure that only authorized users can access student records. (3 Marks)			
Module IV				
Qn No.	Question	Marks	CO	BL
15	A cyber criminal gains unauthorized access to sensitive data, and investigators rely on digital evidence collected from multiple systems to establish the facts of the case. Describe the importance of proper evidence collection and preservation in cyber forensic investigations.	9	4	L2
OR				
16	Explain the concept of chain of custody and discuss its significance in maintaining the integrity of digital evidence.	9	4	L2