COURSE HANDOUT

FOUNDATIONS OF CYBER SECURITY (COM-303)

CSE (Cyber Security) - 3RD SEMESTER

ACADEMIC YEAR (2024-25)

Mr. Arsalan Manzoor Zargar

Assistant Professor

Department of Computer Science and Engineering

Department of Computer Science and Engineering

Model Institute of Engineering & Technology (Autonomous)

Kot Bhalwal, Jammu - 181122

www.mietjmu.in

Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
COM-303	Foundations of Cyber Security	PCC	4	3	1	0	50	100	150

COURSE OUTCOMES

At the end of the course the student will be able to:	
CO1	Explain cyber security principles to secure network and information systems.
CO2	Analyze cyber-attack techniques to improve defensive strategies.
CO3	Evaluate exploitation techniques to prevent and mitigate vulnerabilities.
CO4	Design strategies to defend against advanced persistent threats and malicious code.
CO5	Create incident response plans and perform forensic analysis to handle security breaches.

Unit-I

Cyber Security Introduction: Computer Security, Threats, Harm, Vulnerabilities, Controls, Authentication, Access Control. **Cryptography:** Problems Addressed by Encryption, Terminology. **DES:** The Data Encryption Standard. **AES:** Advanced Encryption System, Public Key Cryptography, Digital Signatures.

(8 Hours)

Unit-II

Programs and Programming: Unintentional (Non-malicious) Programming Oversights, Malicious Code – Malware, Countermeasures. **Web Security:** User Side, Browser Attacks, Web Attacks Targeting Users, Obtaining User or Website Data, Email Attacks. **Operating Systems Security:** Security in Operating Systems, Security in the Design of Operating Systems, Rootkit.

(10 Hours)

Unit-III

Network Security: Network Concepts, Threats to Network Communications, Wireless Network, Security, Denial of Service, Distributed Denial-of-Service. **Strategic Defenses:** Security, Countermeasures, Cryptography in Network Security, Firewalls, Intrusion Detection and Prevention Systems, Network Management.

(8 Hours)

Unit- lV

Cloud Computing and Security: Cloud Computing Concepts, Moving to the Cloud, Cloud Security, Tools and Techniques. Cloud Identity Management, Securing IaaS. **Privacy:** Privacy Concepts, Privacy Principles and Policies, Authentication and Privacy, Data Mining, Privacy on the Web, Email Security, Privacy Impacts of Emerging Technologies.

(10 Hours)

Unit-V

Management and Incidents: Security Planning, Business Continuity Planning, Handling Incidents, Risk Analysis, Dealing with Disaster. **Legal Issues and Ethics:** Protecting Programs and Data, Information and the Law, Rights of Employees and Employers, Redress for Software Failures, Computer Crime, Ethical Issues in Computer Security, Incident Analysis with Ethics.

(8 Hours)

Textbooks

S. No	Name of the Books	Name of the Author	Publisher Name	Edition (Pub.Yr.)
1	Security in Computing	Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies	Prentice Hall	5th (2018)

Reference Books

S. No.	Name of the Books	Name of the Author	Publisher Name	Edition (Pub.Yr.)
1	Information Security: The Complete Reference	Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos D. Keromytis	McGraw Hill	3rd (2017)
2	Information Security: Management Handbook	Harold F. Tipton, CISSP, Micki Krause, CISSP	CRC Press	6th (2007)

COURSE PLAN		
Unit-I - Cyber Security Introduction		
S. No	**Topics**	**Recommended Books**
1	Computer Security, Threats, Harm, Vulnerabilities	Textbook, Chapter 1
2	Controls, Authentication, Access Control	Textbook, Chapter 1
3	**Cryptography:** Problems Addressed by Encryption, Terminology	Textbook, Chapter 2
4	**DES:** The Data Encryption Standard	Textbook, Chapter 2
5	**AES:** Advanced Encryption System	Textbook, Chapter 2
6	Public Key Cryptography	Textbook, Chapter 2
7	Digital Signatures	Textbook, Chapter 2
Unit-II - Programs and Programming		
8	Unintentional (Non-malicious) Programming Oversights	Textbook, Chapter 3
9	Malicious Code – Malware, Countermeasures	Textbook, Chapter 3
10	**Web Security:** User Side, Browser Attacks, Web Attacks Targeting Users	Textbook, Chapter 4
11	Obtaining User or Website Data, Email Attacks	Textbook, Chapter 4
12	**Operating Systems Security:** Security in Operating Systems,	Textbook, Chapter 5
13	Security in the Design of Operating Systems, Rootkit	Textbook, Chapter 5
Unit-III - Network Security		
14	Network Concepts, Threats to Network Communications	Textbook, Chapter 6
15	Wireless Network, Security, Denial of Service, Distributed Denial-of-Service	Textbook, Chapter 6
16	**Strategic Defenses:** Security, Countermeasures, Cryptography in Network Security	Textbook, Chapter 6
17	Firewalls, Intrusion Detection and Prevention Systems,	Textbook, Chapter 6
18	Network Management	Textbook, Chapter 6
Unit-IV - Cloud Computing and Security		
19	**Cloud Computing and Security:** Cloud Computing Concepts, Moving to the Cloud	Textbook, Chapter 8
20	Cloud Security, Tools and Techniques, Cloud Identity Management, Securing IaaS	Textbook, Chapter 8
21	**Privacy:** Privacy Concepts, Privacy Principles and Policies Authentication and Privacy	Textbook, Chapter 9
22	Data Mining, Privacy on the Web,	Textbook, Chapter 9

23	Email Security, Privacy Impacts of Emerging Technologies	Textbook, Chapter 9
Unit-V - Management and Incidents		
24	**Management and Incidents:** Security Planning, Business Continuity Planning	Textbook, Chapter 10
25	Handling Incidents, Risk Analysis, Dealing with Disaster.	Textbook, Chapter 10
26	**Legal Issues and Ethics:** Protecting Programs and Data, Information and the Law	Textbook, Chapter 11
27	Rights of Employees and Employers, Redress for Software Failures, Computer Crime	Textbook, Chapter 11
28	Ethical Issues in Computer Security, Incident Analysis with Ethics	Textbook, Chapter 11

ADDITIONAL WEB RESOURCES

1.	**MOOCs:** 1. Introduction to Computers and Operating Systems and Security | Microsoft 2. Cybersecurity Threat Vectors and Mitigation | Microsoft 3. Cybersecurity Identity and Access Solutions using Azure AD | Microsoft 4. Foundations of Cybersecurity | Google
2.	**YouTube:** 1. Cyber Security Full Course | Simplilearn

GRADING AND ASSESSMENT

- **Sessional Test**: 20 marks
- **Assignment**: 20 marks
- **Attendance**: 10 marks
- **Final Examination**: 100 marks

COURSE POLICIES

- **Attendance**: Minimum 75% attendance is mandatory to appear in the final examination of the course.
- **Academic Integrity**: MIET's academic integrity policies apply. Plagiarism will not be tolerated.
- **Late Submissions**: Assignments and projects must be submitted by the specified timelines.

FACULTY INFORMATION

- **Office Hours**

  Monday-Friday (02:35 PM - 04:20 PM)
  Saturday (Full Day)

- **Contact Information**
  arsalan.cse@mietjammu.in | +91-7006416585