BCA-6-01T-EC-C2: Cyber Attacks and Counter Measures

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage: 40%

INSTRUCTIONS FOR THE PAPER SETTER/EXAMINER

1. The syllabus prescribed should be strictly adhered to.
2. The question paper will consist of three sections: A, B, and C. Sections A and B will have four questions from the respective sections of the syllabus and will carry 10 marks each. The candidates will attempt two questions from each section.
3. Section C will have fifteen short answer questions covering the entire syllabus. Each question will carry 3 marks. Candidates will attempt any ten questions from this section.
4. The examiner shall give a clear instruction to the candidates to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.
5. The duration of each paper will be three hours.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt any two questions each from the sections A and B of the question paper and any ten short questions from Section C. They have to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.

Course Name: Cyber Attacks and Counter Measures **Course Code: BCA-6-01T-EC-C2**	
Course Outcomes (COs) After the completion of this course, the students will be able to:	
CO 1	Understand the importance of a network basics and brief introduction on security of network protocols
CO 2	Demonstrate a solid understanding of foundational cybersecurity concepts, principles, and best practices.
CO 3	Apply risk assessment methodologies to evaluate and prioritize potential vulnerabilities within a given system or network.
CO 4	Design and develop security plans and strategies to ensure the integrity of information in compliance with best practices, relevant policies, standards, and regulations.
CO 5	Evaluate the impact of cybersecurity decisions on privacy, compliance, and organizational reputation, and adhere to ethical standards in the field.

Detailed Contents:

Module No.	Module Name	Module Contents
Section-A		
Module 1	**Introduction to Cybersecurity and Threat Landscape**	• Overview of Cybersecurity: Fundamental concepts, objectives, and importance. • Cyber Threat Landscape: Types of cyber threats, attack vectors, and motivations. • Current Trends: Analysis of recent cyber threats and emerging trends in the cybersecurity landscape.
Module II	**Security Fundamentals and Risk Assessment**	• Security Foundations: Principles, protocols, and standards in cybersecurity. • Vulnerability Assessment: Techniques for identifying and assessing vulnerabilities. • Risk Management: Understanding risk, assessing potential impacts, and prioritizing security measures.
Section-B		
Module III	**Implementing Security Measures and Incident Response**	• Security Controls: Designing and implementing security measures, including firewalls, antivirus, encryption, and access controls. • Incident Response Planning: Developing and implementing an incident response plan. • Security Monitoring: Using tools and techniques to monitor for potential security incidents.
Module IV	**Ethical Hacking, Penetration Testing, and Legal Considerations**	• Ethical Hacking: Introduction to ethical hacking principles and practices. • Penetration Testing: Conducting controlled attacks to identify and address vulnerabilities. • Legal and Ethical Considerations: Understanding the legal and ethical aspects of cybersecurity, including compliance, privacy, and responsible disclosure.

Books

1. Sammons, John, and Michael Cross, "The basics of cyber safety: computer and mobile device safety made easy", Syngress
2. Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies, "Security in Computing", Pearson
3. Brooks, Charles J., Christopher Grow, Philip Craig, and Donald Short, "Cybersecurity essentials", Sybex

4. William Stallings "Network Security Essentials", Pearson
5. Ross J. Anderson "Security Engineering: A Guide to Building Dependable Distributed Systems", 2nd Ed., John Wiley & Sons