Avinashilingam Institute for Home Science and Higher Education for Women
Deemed to be University Estd. u/s 3 of UGC Act 1956, Category 'A' by MHRD (now MoE)
Re-accredited with 'A++' Grade by NAAC. CGPA 3.65/4, category I by UGC
Coimbatore - 641 043, Tamil Nadu, India

Bachelor's Degree Examination – May 2025
VI Semester

Class : III UG
Major : Computer Applications

Time : 3 Hours
Max. Marks: 100

21BCAC31 Cyber Security

Course Outcomes:
CO1: Identify various types of cyber-attacks, tools used for gathering information about target.
CO2: Assess different types of cyber criminals and the motives behind them.
CO3: Realize the exploitations and the malicious codes to be precautious.
CO4:: Analyze the defense techniques suitable for the system.
CO5:: Apply the techniques for securing the systems.

Part A **10 x 1 = 10**
Choose the Correct Answer

1. Which of the following is an example of a cryptographic algorithm used to ensure data confidentiality? CO1K1
   a. SHA-256 b. RSA c. AES d. TCP/IP

2. What is the main purpose of a firewall in network security? CO1K2
   a. To encrypt data
   b. To monitor network traffic and block unauthorized access
   c. To store sensitive data securely
   d. To improve the speed of the network

3. Which of the following is an example of phishing? CO2K2
   a. Sending unsolicited emails asking for login credentials
   b. Hacking a website to steal credit card information
   c. Installing a Trojan on a victim's machine
   d. Compromising a router's firmware

4. What is a common goal of an attacker using antiforensic techniques? CO2K1
   a. To install malware on a victim's machine
   b. To delete logs and cover their tracks
   c. To encrypt sensitive data
   d. To enhance the security of a network

5. Which type of vulnerability is commonly exploited by an attacker to run arbitrary code in a system? CO3K2
   a. Buffer overflow
   b. SQL Injection
   c. Cross-Site Scripting (XSS)
   d. Format string vulnerability

6. What does SQL Injection allow an attacker to do? CO3K1
   a. Gain unauthorized access to a database
   b. Inject malicious code into a web server
   c. Steal users' cookies
   d. Launch denial-of-service attacks

7. Which of the following is an example of self-replicating malicious code? CO4K2
   a. Virus b. Trojan c. Worm d. Spyware

8. What is a rootkit designed to do? CO4K1
   a. Encrypt data
   b. Provide unauthorized access to a system while hiding its presence
   c. Steal passwords
   d. Monitor network traffic

9. What is the primary purpose of a honeypot in cybersecurity? CO5K1
   a. To deceive attackers into thinking they've found a real target
   b. To encrypt sensitive data
   c. To block malware
   d. To monitor network traffic

10. Which of the following is used for automated analysis of malicious code? CO5K2
    a. Antivirus software
    b. Honeypots
    c. Intrusion detection systems
    d. Sandboxing

Part B **5 x 6 = 30**

Answer ALL questions

Each answer should not exceed 400 words or two pages

11.a. Explain the basic principles of cryptography and how they contribute to securing data. CO1K2

(or)

11.b. Describe the role of firewalls in protecting a network and provide an example of a firewall configuration. CO1K2

12.a. Illustrate the concept of phishing and how it is used in cyberattacks. CO2K3

(or)

12.b. What are the main types of mobile malicious code and how do they affect users? CO2K3

13.a. Explain what a buffer overflow vulnerability is and how attackers exploit it. CO3K4

(or)

13.b. What is SQL Injection and how can it compromise the security of a website? CO3K4

14.a. Appraise the concept of persistent software techniques and their impact on cyber security CO4K4

(or)

14.b What is a rootkit and how does it compromise system security? CO4K4

15.a. Explain how memory forensics is used to detect malware in a system. CO5K2

(or)

15.b. What are Intrusion Detection Systems (IDS) and how do they contribute to network security? CO5K2

Part C **5 x 12 = 60**

Answer ALL questions

Each answer should not exceed 800 words or four pages

16.a. Describe the concept of Information Assurance and its components in securing data. CO1K2

(or)

16.b. Discuss the key security principles of Microsoft Windows and how they are implemented to protect a system. CO1K2

17.a. Examine the fraud techniques Phishing, Smishing, Vishing and their potential impact on users. CO2K3

(or)

17.b. Demonstrate the concept of rogue antivirus software and its potential risks. CO2K3

18.a. Appraise the concept of shellcode and how it is used in exploitation. CO3K4

(or)

18.b. Analyze how a format string vulnerability works and provide an example of its exploitation. CO3K4

19.a. Illustrate the working of self-replicating malicious code and provide examples. CO4K3

(or)

19.b. Discover how malicious code targeting privileged user accounts can escalate privileges and cause severe damage. CO4K3

20.a. Appraise the concept of honeypots and how they are used to detect and analyze Cyber attacks. CO5K5

(or)

20.b. Evaluate how automated malicious code analysis systems work and their role in cyber security defense. CO5K5