



K. Sambath

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

Continuous Internal Assessment Test I – February 2026

VI Semester

Class : III UG (2019 & 2022 Repeaters)
Major : Computer Applications

Time: 2 hours
Maximum Marks: 60

18BCAC31/21BCAC31 Cyber Security

Course Outcomes:

At the end of the course, students will:

1. Identify various types of cyber attacks, tools used for gathering information about target.
2. Assess different types of cybercriminals and the motives behind them.
3. Realize the exploitations and malicious code to be precautions.
4. Analyze the defense techniques suitable for the system.
5. Apply the techniques for securing the systems.

Part - A

6 x 1 = 6

Choose the Correct Answer

1. A cryptographic key is used to:
a. Open network ports
b. Encrypt and decrypt data
c. Identify IP addresses
d. Monitor traffic
CO1 K1
2. Which of the following is an advantage of a firewall?
a. Prevents all cyberattacks
b. Provides access control
c. Eliminates need for encryption
d. Speeds up the internet
CO1 K1
3. Which medium is most commonly used for phishing attacks?
a. SMS
b. Email
c. Phone calls
d. Bluetooth
CO2 K1
4. Rogue antivirus programs are also known as
a. Spyware
b. Scareware
c. Adware
d. Ransomware
CO2 K2
5. A format string vulnerability occurs due to:
a. Improper input validation
b. Incorrect SQL queries
c. Unchecked user-supplied format strings
d. Weak passwords
CO3 K1
6. An integer overflow occurs when
a. A string exceeds its buffer size
b. A calculation exceeds the maximum integer value
c. A program crashes due to syntax error
d. Memory is not allocated
CO3 K2

Part - B

3 x 6 = 18

Answer ALL Questions

Each answer should not exceed 400 words or two pages

7. a. Explain in detail cryptography. (or) CO1 K1
7. b. Discuss about tokens and messages. CO1 K2
8. a. Write in detail about click fraud with example. (or) CO2 K2
8. b. Describe about threat infrastructure. CO2 K2
9. a. Write in detail about shell code. (or) CO3 K2
9. b. Explain about integer overflow vulnerabilities. CO3 K2

Part - C

3 x 12 = 36

Answer ALL questions

Each answer should not exceed 800 words or four pages

10. a. Discuss in brief about Information assurance fundamentals. (or) CO1 K1
10. b. Explain in detail about Firewall and its uses. CO1 K1
11. a. Explain in detail about Phishing and Smishing with an example. (or) CO2 K1
11. b. Discuss about mobile malicious code with example. CO2 K1
12. a. Describe in detail about format string vulnerabilities. (or) CO3 K1