Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 09/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CSA4713 **Course Name:** Cyber Security Testing

Semester: Third Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	46	44

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Define "Cybersecurity" and list the three pillars of the CIA Triad.	2	CO1	BT1
2	Explain the purpose of "Retesting" in the security testing lifecycle.	2	CO2	BT2
3	Apply the concept of "Boundary Value Analysis" to test a login page that requires a password length between 8 and 16 characters.	2	CO1	BT3
4	Define the term "Attack Surface" and give two examples of attack vectors.	2	CO2	BT1
5	Differentiate between a "Vulnerability" and a "Threat" using a house analogy.	2	CO1	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Explain the four pillars of security: Confidentiality, Integrity, Availability, and Non-Repudiation. Provide one mechanism used to enforce each.	10	CO1	BT2
7	Apply the concept of Symmetric and Asymmetric encryption to explain how a hybrid encryption system (like HTTPS/TLS) securely transmits data over the internet.	10	CO1	BT3

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Analyze the differences between Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). Justify which model is best suited for a large financial institution.	10	CO1	BT4
9	Evaluate the effectiveness of Multi-Factor Authentication (MFA) as a security control. Discuss its limitations and how attackers bypass it (e.g., MFA fatigue).	10	CO1	BT6

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the concept of "Information Gathering" in the security testing lifecycle. Discuss the difference between passive and active reconnaissance, and provide two examples of tools used for each.	10	CO2	BT2
11	Explain the purpose of "Validation" in the security testing lifecycle. Why is it important to manually validate findings from a vulnerability scanner?	10	CO2	BT2

PART E: Answer Any 1 Following Questions. 10 M

PTO (Please Turn Over)

Q.N.	Questions	M	CO	BT
12	Apply the concept of "Black-Box Testing" to a login page of a banking application. Describe the specific test cases you would design using Equivalence Partitioning and Boundary Value Analysis.	10	CO2	BT3
13	Explain the "Security Testing Lifecycle." Describe the phases of Planning, Information Gathering, Threat Modeling, and Vulnerability Identification in detail.	10	CO2	BT2