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

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

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: 05/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CCS3405 **Course Name:** Vulnerability Assessment and Penetration Testing

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

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	20	22	6	22	20

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Why is vulnerability assessment important in a SCADA environment?	2	CO3	BT2
2	Mention two potential impacts of SSI injection.	2	CO4	BT1
3	How can Nmap identify open ports?	2	CO3	BT2
4	What is a false positive in vulnerability assessment? Give Example	2	CO3	BT1
5	Differentiate between active and passive information gathering.	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Explain the different phases of penetration testing in detail. Discuss the activities performed during information gathering, scanning, vulnerability assessment, exploitation, post-exploitation, and reporting.	10	CO1	BT4
7	Explain the different categories of penetration testing. Compare black-box, white-box, and gray-box testing with suitable examples.	10	CO1	BT4

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Explain active and passive information gathering techniques. Discuss their approaches, sources of information, advantages, and limitations with suitable examples	10	CO2	BT4
9	Explain host discovery and port scanning techniques. Discuss how Nmap can be used to identify live hosts, open ports, services, and operating systems.	10	CO2	BT3

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the challenges and considerations involved in vulnerability assessment of a SCADA environment. Discuss why active scanning must be carefully controlled in industrial control systems.	10	CO4	BT4
11	Explain the architecture of Software-Defined Networking (SDN). Discuss the data plane, control plane, and application plane and identify the major security concerns associated with each plane.	10	CO4	BT4

PTO (Please Turn Over)

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	Explain Cross-Site Scripting (XSS) vulnerability. Discuss stored XSS, reflected XSS, and DOM-based XSS, along with their impacts and prevention techniques.	10	CO5	BT4
13	Explain Server-Side Includes (SSI) and SSI injection. Describe how an application can be tested for SSI injection and discuss appropriate mitigation techniques.	10	CO5	BT3