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: 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	Vulnerability assessment is important in a SCADA environment because it helps **identify security weaknesses in industrial control systems, devices, and network services** before they can be exploited. It helps protect **system availability, integrity, safety, and critical industrial operations** from cyber threats.	2	CO3	BT2
2	Any **two** of the following: 1. **Unauthorized execution of server-side commands or directives**, depending on the server configuration. 2. **Disclosure of sensitive information** such as server files or application data. 3. **Modification of dynamically generated web-page content.** 4. **Unauthorized access or compromise of the web application/server.**	2	CO4	BT1
3	• Nmap sends appropriate **TCP or UDP probes** to specified ports. • It analyzes the responses to determine whether the ports are **open, closed, or filtered**.	2	CO3	BT2
4	A **false positive** occurs when a vulnerability scanner **reports a security vulnerability that does not actually exist** on the target system. **Example:** A scanner reports that a web server is vulnerable to a particular attack based on its detected version, but manual verification shows that the vulnerability has already been patched.	2	CO3	BT1
5	Active Information Gathering Directly interacts with the target system or network. More likely to be detected or logged by the target. Example: **port scanning using Nmap**. Passive Information Gathering Collects information without directly interacting with the target. Generally less likely to be detected. Example: **search engines, public websites, WHOIS, and social media**.	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT

ANSWER KEY

PTO (Please Turn Over)

6	**Information Gathering** Collect information about the target, such as domains, IP addresses, hosts, technologies, and services using active and passive reconnaissance. Scanning Identify live hosts, open ports, running services, service versions, and operating-system information using appropriate scanning techniques. Vulnerability Assessment Analyze discovered services and configurations to identify potential vulnerabilities and assess their severity and impact. Exploitation & Post-Exploitation With authorization, safely validate identified vulnerabilities and determine their potential impact while documenting the evidence obtained. Reporting Document findings, evidence, risk levels, affected systems, and suitable remediation recommendations in a penetration-testing report.	10	CO1	BT4
7	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	host discovery and port scanning techniques. 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	vulnerability assessment of a SCADA environment. Discuss why active scanning must be carefully controlled in industrial control systems.	10	CO4	BT4
11	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

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	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	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

ANSWER KEY