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: 07/10/2026 **Time:** 09:30 AM - 11:00 AM

Course Code: IST2505 **Course Name:** Ethical Hacking

Semester: Fifth 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	Distinguish between Grey Hat and White Hat hackers.	2	CO1	BT2
2	Define the term 'Exploit' with a suitable example.	2	CO1	BT1
3	Differentiate between the MX and NS DNS record types	2	CO1	BT2
4	Describe what is meant by Google Dorking (Google Hacking).	2	CO2	BT2
5	Summarize the key sources typically used in passive information gathering	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Compare the roles of Black Hat, White Hat and Grey Hat hackers, and justify why White Hat hacking is considered legal.	10	CO1	BT2
7	Describe the security services defined under the X.800 standard — Authentication, Access Control, Data Confidentiality, Data Integrity and Non-repudiation.	10	CO1	BT2

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Explain the NIST penetration testing methodology and describe its four phases.	10	CO1	BT2
9	Describe the OWASP penetration testing methodology and explain the purpose of its seven phases.	10	CO1	BT2

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Illustrate WHOIS lookup and describe the impact of GDPR on the information available through WHOIS records.	10	CO2	BT3
11	Demonstrate how a social engineer could manipulate an employee into revealing sensitive information using the six principles of persuasion.	10	CO2	BT3

PART E: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT

12	Interpret the structured five-step footprinting methodology used by ethical hackers to organise reconnaissance activities.	10	CO2	BT3
13	Examine the role of OSINT tools such as Shodan and SpiderFoot in gathering intelligence about a target organisation.	10	CO2	BT3