24MCPE651

MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING

(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

Model Question Paper

Third Semester MCA Degree Examination, 2025-26

ETHICAL HACKING

Time: 3 Hours **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.

		Module -1	M	L	C
Q1	a.	You are assigned to conduct a penetration test for a college management system. Demonstrate how you will proceed from pre-engagement to reporting.	10	L3	CO1
	b.	A file named report.txt is stored in /home/kali/Reports. You are asked to copy this file to /home/kali/Submission. Then move the original file to /home/kali/OldReports. After the evaluation is completed, delete the file from /home/kali/OldReports. Write the commands and explain their purpose.	10	L3	CO1
		OR			
Q2	a.	You are the system administrator of a Kali Linux lab. A new student named SUMAN joins the lab. Give the commands to: • Create a new user named SUMAN • Switch to the SUMAN account • Create a directory named Practicals inside the home folder • Create a file named task1.txt inside Practicals • Delete the file task1.txt • Delete the directory Practicals • Explain the purpose of each command.	10	L3	CO1
	b.	A file named student.txt is to be created in /home/kali. a) Write the command to write "Name: Rahul" into the file. b) Write the command to append "Course: MCA" into the same file. c) Add one more line "Semester: 2" without deleting previous content. d) Show the contents of the file. e) Explain how > and >> work in file handling.	10	L3	CO1
		Module- 2			
Q3	a.	Given a target machine, show how you will use Kali Linux tools for information gathering and vulnerability scanning.	10	L3	CO2
	b.	You are assigned to perform advanced network scanning using Nmap. Explain how you would utilize the Nmap Scripting Engine to detect vulnerabilities on multiple hosts. Illustrate your approach with examples	10	L3	CO2

		of specific NSE scripts and describe how they enhance the scanning process.			
OR					
Q4	a.	You have been tasked with conducting a vulnerability assessment of the internal network. Describe the steps you would take to create and configure Nessus scanning policies specifically for internal systems. How you would carry out scans across multiple devices efficiently using Nessus, and detail the process of exporting and saving the scan results for documentation and analysis. Finally, discuss how the information obtained from these scans can be used to identify security weaknesses and strengthen the overall security posture of the network.	10	L3	CO2
	b.	A company gives you the domain name example.com to perform initial reconnaissance. a) How you will use Netcraft to collect information about the website. b) Show how Whois Lookup helps in finding domain ownership details. c) Explain how DNS reconnaissance can be performed for this domain. d) Explain how you will search for email addresses related to this domain.	10	L3	CO2
Module- 3					
Q5	a.	You have identified that a web server is running WebDAV with default credentials. Write your answers for the following: a) List down the steps you would follow to exploit this vulnerability using Metasploit. b) Throw some light on how you would choose an appropriate payload and deliver it to the target system. c) How would you execute a script on the compromised web server after successful exploitation. d) Write a brief on the methods you would use to maintain persistent access to the target system.	10	L3	CO3
	b.	You are asked to perform a complete client-side attack simulation. Describe how you would plan the attack, deliver the payload using HTTP/HTTPS, and explain how you would use the results to improve user security awareness.	10	L3	CO3
OR					
Q6	a.	You are asked to identify users who may be vulnerable to malicious links. How will you conduct a client-side exploitation test using HTTP/HTTPS payloads. What suitable security measures would you recommend after obtaining the results of the test.	10	L3	CO3
	b.	You are assigned to evaluate the strength of user passwords in an organization's network. Describe the procedure you would follow to carry out password attacks in a controlled environment. How you would use Metasploit or other appropriate tools to perform these attacks. Further, describe how you would analyze the results to identify weak or easily guessable passwords.	10	L3	CO3
Module – 4					
Q7	a.	An organization wants to test its defenses against mass email attacks. Describe how you would plan and execute a mass mailing attack and	10	L3	CO4

		explain how you would measure its success rate.			
	b.	During a security assessment, you are asked to check whether users can be fooled by fake websites. Describe how you would create and deploy a fake website and analyze how user interaction with it can be used to improve security awareness.	10	L3	CO4
OR					
Q8	a.	After completing a social engineering test, you are asked to prepare a report. Describe how you would analyze the results from phishing, spoofing, and fake website attacks and recommend suitable security controls.	10	L3	CO4
	b.	A company is concerned that its email domain might be vulnerable to spoofing attacks. As a security analyst, explain how you would investigate this issue by first identifying the organization's mail server using DNS lookup techniques. Then, describe how you would interact with the SMTP server to test its behavior and analyze whether it allows spoofed emails to be sent. Based on your observations, explain how you would conclude whether the domain is vulnerable to email spoofing or not.	10	L3	CO4
MODULE 5					
Q9	a.	During penetration testing, you find a parameter that seems to execute system-level commands. Describe how you would verify a Command Execution vulnerability and analyze how this could lead to complete system compromise.	10	L3	CO5
	b.	While testing a website, you notice that it loads pages using a URL parameter. Describe how you would check whether the application is vulnerable to Local File Inclusion (LFI) and analyze what kind of sensitive information could be exposed.	10	L3	CO5
OR					
Q10	a.	After identifying SQL Injection in one module and XPath Injection in another, illustrate how you would analyze their severity and prioritize which vulnerability should be fixed first and why?	10	L3	CO5
	b.	A banking web application allows users to transfer money without asking for the password again. How you would test whether this application is vulnerable to CSRF and analyze the possible impact of such an attack.	10	L3	CO5