


Name:			
Enrolment No:			
<div><div>UPES</div><div>End Semester Examination, May 2025</div></div>			
Programme Name: MCA		Semester : II	
Course Name : Penetration Testing & Ethical Hacking		Time : 03 hrs.	
Course Code : CSCS7014_4		Max. Marks: 100	
Nos. of page(s) : 2			
Instructions: Please attempt according to the time provided and given weightage.			
<div>SECTION A</div> <div>(20 Marks) 5 Questions – Each 4 Marks-No Choice-Attempt all Questions</div>			
S.No.	Question	Marks	CO
Q 1	Compare HTTP and HTTPS in detail. Include differences in security, encryption, and data transfer.	4	CO1
Q 2	Upon scanning, you discover that ports 21 and 443 are open on the windows server. Explain the role of these ports and their associated protocols.	4	CO2
Q 3	What is the difference between Boolean-based and Time-based SQL Injection?	4	CO3
Q 4	What is the OWASP Top 10 and mention any four OWASP Top 10 vulnerabilities.	4	CO4
Q 5	List any four differences between WEP, WPA, WAP2 and WAP3 protocols.	4	CO1
<div>SECTION B</div> <div>(40 Marks) 5 Questions-Each 10 Marks-One Choice-Attempt any 4 questions out of 5</div>			
Q 6	Describe the complete step-by-step process for cracking a WPA/WPA2 Wi-Fi password using ethical hacking tools. Include all the necessary commands used in each phase.	10	CO1
Q 7	What is Burp Suite? Describe the functions and significance of its components: Proxy, Intruder, Repeater, Decoder, and Comparer. Give examples of how each component is used during a web application penetration test	10	CO2
Q 8	Explain Directory Traversal Attacks in web applications. How do different security levels (low, medium, high, impossible) impact these attacks in vulnerable web apps like DVWA? Also, describe how Null Byte Injection and Base64 Encoding techniques can bypass certain security configurations.	10	CO4
Q 9	Explain the working and application of Hashcat as a password cracking tool. Discuss the different attack modes supported by Hashcat and provide examples of scenarios where each mode can be effectively used. OR Discuss the various techniques of password cracking in ethical hacking. Compare Brute Force, Dictionary, Rainbow Table, Phishing, and Hybrid attacks in terms of methodology, effectiveness, use cases, and limitations.	10	CO3

SECTION C

(40 Marks) 2 Questions -Each 20 Marks- One Choice-Attempt any 2 questions out of 3

Q 10	<p>Describe how to conduct Active Footprinting in Ethical Hacking. Explain how to use Nmap for identifying:</p> <ul style="list-style-type: none">• Live hosts in a network• Open ports on a target system• Operating system fingerprinting• Version detection of running services <p>And also provide a comparative explanation of the following scanning types use.</p> <ul style="list-style-type: none">• Ping Scan• ARP Scan• Port Scan	20	CO4
Q11	<p>What is SQL Injection? Describe the various types of SQL Injection attacks, their potential impacts on web applications and databases, and discuss the techniques and best practices to prevent such attacks</p> <p>OR</p> <p>Explain the complete process of using SQL Map to perform a penetration test on a web application. Your answer should include:</p> <ol style="list-style-type: none">1. Basic SQL Map commands to identify databases, tables, columns, and dump data2. How to use SQL Map with session cookies in authenticated environments like DVWA3. Explain the advanced SQL Map features such as --risk, --level, --technique, --batch, --verbosity, and --threads4. How to use SQL Map with HTTP logs, Google Dorks, and bulk request files	20	CO5