

CBCS SCHEME

USN

MMCH311A

Third Semester MCA Degree Examination, June/July 2026

Ethical Hacking

Time: 3 hrs.

Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.

2. M : Marks, L: Bloom's level, C: Course outcomes.

Module – 1				M	L	C
Q.1	a.	Define Ethical Hacking and explain its importance in cyber security.		5	2	1
	b.	Explain legal and ethical considerations involved in ethical hacking.		7	2	1
	c.	Differentiate between Black Hat, White Hat, and Grey Hat hackers.		8	2	1
OR						
Q.2	a.	Explain Red Team, Blue Team, and Purple Team concepts.		10	2	1
	b.	Explain common cyber security terminologies used in ethical hacking.		5	2	1
	c.	Describe Zero-day vulnerabilities and their impact on organizations.		5	2	1
Module – 2						
Q.3	a.	Define passive and active information gathering techniques.		7	2	2
	b.	Explain WHOIS lookup and its role in footprinting.		7	3	2
	c.	Write and explain six Google hacking dorks used in vulnerability discovery.		6	2	2
OR						
Q.4	a.	Explain Open Source Intelligence (OSINT) techniques.		5	2	2
	b.	Explain DNS enumeration using NSLOOKUP with suitable commands.		10	3	2
	c.	Explain social engineering and its common attack methods.		5	2	2
Module – 3						
Q.5	a.	Explain different port scanning techniques used in ethical hacking.		10	2	3
	b.	Explain service enumeration and version detection.		10	2	3
OR						
Q.6	a.	Apply SYN, TCP, and UDP scanning using NMAP with commands.		10	3	3
	b.	Explain TCP/IP three-way handshake and the role of RST packet in scanning.		10	2	3
Module – 4						
Q.7	a.	Explain password cracking techniques and tools.		8	3	4
	b.	Describe Trojan Horse malware and its countermeasures.		5	3	4
	c.	Explain privilege escalation and its impact on system security.		7	3	4
OR						
Q.8	a.	Explain brute-force and password spraying attacks with differences.		10	2	4
	b.	Explain common malware types and their countermeasures.		10	2	4
Module – 5						
Q.9	a.	Differentiate between IDS and IPS.		5	2	5
	b.	Explain common web application vulnerabilities.		5	2	5
	c.	Explain SQL Injection and Cross-Site Scripting (XSS) with examples..		10	2	5
OR						
Q.10	a.	Explain different types of Intrusion Detection Systems.		5	2	5
	b.	Explain MAC flooding and ARP poisoning attacks.		8	2	5
	c.	Explain honeypots and compare them with IDS.		7	2	5
