COURSE MODULE: ETHICAL HACKING

Course Coordinator: Prof. Yeshashwini Bhandari K R				Academic Year:**2025-26**	
Program: Master of Computer Applications					
Course Code	**Course Title**	**Core/Elective**	**Prerequisite**	**Contact Hours** L: T: P:S	**Total Hrs/ Sessions**
MMCH311A	**ETHICAL HACKING**	**PEC**	OS, CN, Basic Information Security Concepts	3:0:0	40

Course Learning Objective:

The course will enable the students to:

- To develop a comprehensive understanding of ethical hacking principles, methodologies, and tools, and recognize the significance of ethical and legal considerations in conducting security assessments.
- To acquire hands-on proficiency in executing penetration tests, vulnerability assessments, and Ethical hacking techniques across various system components, networks, and applications.
- To demonstrate the ability to identify, assess, and prioritize vulnerabilities in diverse computing Environments using both manual and automated methods and effectively communicate these findings to stakeholders.
- To develop a strategic mindset towards cyber security by acquiring knowledge of common attack Vectors, learning to simulate real-world attacks, and implementing preventive measures to secure, systems Networks and web applications.

Teaching-Learning Process:

This teaching–learning process ensures that students:

- Gain a strong conceptual and ethical foundation in cyber security
- Develop practical skills in ethical hacking and penetration testing
- Build analytical, strategic, and communication abilities required for real-world cyber security roles

Module-1

Introduction to Ethical Hacking

Introduction to ethical hacking and its importance, Legal and ethical considerations in ethical hacking, Differentiating between black hat, white hat, and grey hat hacking, Basic cyber security concepts and terminology, Overview of penetration testing methodologies.

Module-2

Foot printing and Information Gathering

Passive and active information gathering techniques, Who is lookup, DNS enumeration, and social engineering, Tools and methodologies for foot printing, Google hacking and OSINT (Open-Source Intelligence) techniques.

Module-3

Scanning and Enumeration: Port scanning techniques: SYN,TCP,UDP scans; Service enumeration and version detection; NetBIOS, SNMP, and SMTP enumeration; Vulnerability scanning and assessment.

Module-4

System Hacking and Exploitation

Password cracking techniques and tools; Privilege escalation and maintaining access; Malware types And counter measures; Exploiting common vulnerabilities(e.g.,bufferoverflow, SQLinjection)

Module-5
Web Application and Network Security Common web vulnerabilities: SQL injection, XSS, CSRF; Web application penetration testing methodology; Network sniffing and spoofing; Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
Assessment Details (both CIE and SEE) The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together. **Continuous Internal Evaluation:** 1. Two Unit Tests each of 25 Marks 2. Two assignments each of 25 Marks or one Skill Development Activity of 50 marks to attain the COs and POs The sum of two tests, two assignments/skill Development Activities, will be scaled down to 50 marks CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course. **Semester-End Examination:** 1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50. 2. The question paper will have ten full questions carrying equal marks. 3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module. 4. Each full question will have a sub-question covering all the topics under a module. 5. The students will have to answer five full questions, selecting one full question from each module
List of Textbooks 1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRCPress, 2015, ISBN978-1- 4822-3161-8(Paperback) 2. Harper Allen, Gray Hat Hacking: The Ethical Hackers HandBook, 3rd Edition, McGrawHill, 2011. 3. Jay Beale ,AndrewR. Baker, Joel Esler, Snort Intrusion Detection and Prevention Toolkit, Syngress Publishing, Inc,2007, ISBN-13:978-1-59749-099-3 4. William Stallings, Network Security Essentials: Applications and Standards, Pearson Education Limited 2017, ISBN13:978-1-292-15485-5 5. Patrick Engebretson, The Basics of Hacking and Penetration Testing, Syngress Publishing,2013, ISBN978-0-12-411644-3
Web links and Video Lectures (e-Resources): Nmap-Official Documentation : https://nmap.org/book/ https://nvd.nist.gov/
Skill Development Activities Suggested: The students, with the help of the course teacher, can take up Java-related technical activities such as coding exercises, mini projects, and problem-solving tasks, or interact with industry to identify problems for study in the form of research, testing, or projects. Creative and innovative solutions should be attempted, and the prepared report shall be evaluated for CIE marks.

Course Outcomes: At the end of the course, the student will be able to:		
COs	**Description**	**RBTL**
CO1	Explain the core concepts, principles and legal Considerations of ethical hacking.	**L2**
CO2	Make us of different tools and techniques for information gathering, scanning and enumeration	**L3**
CO3	Apply tools and techniques for exploiting vulnerabilities, Network sniffing, web application hacking, system hacking, Escalating privileges, etc.	**L3**
CO4	Analyze the results of IDS/IPS, ethical hacking and penetration testing tasks	**L4**

The Correlation of Course Outcomes (CO's) and Program Outcomes (PO's)

SUBJECT CODE: MMCH311A			TITLE: ETHICAL HACKING		FACULTY: YESHASHWINI BHANDARI K R		
List of Course Outcomes	**Program Outcomes**						
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**
CO-1	1					2		
CO-2	2				2	3		
CO-3	3				2	3		
CO-4	3				3	2	3	
Total								

Note: 3 = Strong Contribution 2 = Average Contribution 1 = Weak Contribution - = No Contribution