Faculty of Engineering & Technology
Master of Technology (M. Tech)
(W. E. F.: 2023-24)

Document ID: SUTEFETM-01

Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Master of Technology (M.Tech.) – Cyber Security
Course Code	:	1MCS04
Course Title	:	Web Application and Penetration Testing
Type of Course	:	Cyber Security
Year of Introduction	:	2023-24

Prerequisite	:	Knowledge in information security and Knowledge on Web Application.
Course Objective	:	Introduce Vulnerability Assessment and Penetration Testing, To be familiar with the Penetration Testing and Tools, To get an exposure to Metasploit exploitation tool, Linux exploitand Windows exploit, To gain knowledge on Web Application Security vulnerabilities, Vulnerability analysis and Malware analysis.
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	Understand social engineering attacks
	CO2	Learn to handle the vulnerabilities of a Web application.
	CO3	Perform penetration testing
	CO4	Analyze the malware type and impact.

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	**T**	**P**	**C**	**SEE**	**CIA**	**SEE**	**CIA**	
3	0	2	4	70	30	30	20	150

Legends: ***L****-Lecture;* ***T****–Tutorial/Teacher Guided Theory Practice;* ***P*** *– Practical,* ***C*** *– Credit,* ***SEE*** *– Semester End Examination,* ***CIA*** *- Continuous Internal Assessment (It consists ofAssignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	Introduction Ethics of Ethical Hacking: Why you need to understand your enemy'stactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.	07	20%	CO1
2	Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.	08	25%	CO2 CO3
3	Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits,Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.	08	20%	CO2 CO3

4	Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of theOWASP Top Ten SQL Injection vulnerabilities,Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.	08	15%	CO2 CO3
5	Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client- side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.	08	20%	CO4

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**20**	**30**	**30**	**20**	**0**	**0**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	Kali Linux OS
2	VMWare
3	Nmap
5	Nikto
6	Burp Suite
7	Wireshark

Suggested Learning Websites

Sr. No.	Name of Website
1	https://www.coursera.org
2	https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/
3	https://www.udemy.com

Reference Books

Sr. No.	Name of Reference Books
1	"Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
2	The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications