Faculty of Computer Science & Applications
Master of Computer Application with Cyber Security
(W. E. F.: 2023-24)

Document ID: SUTEFCAM-01

Name of Faculty	:	Faculty of Computer Science & Applications
Name of Program	:	Master of Computer Application with Cyber Security
Course Code	:	2MCY03
Course Title	:	Ethical Hacking
Type of Course	:	Professional core
Year of Introduction	:	2023-24

Prerequisite	:	Programming Languages, LINUX, Database Engine Skills and most importantly zeal to learn
Course Objective	1	To help students understand how ethical hacking is used as a method to prevent hacking
	2	To make it possible for students to learn the process of identifying vulnerabilities and exploits of the technological ecosystem comprising of various hardware, software, network, OS and applications and identify suitable countermeasures
	3	To facilitate students, appreciate the need for understanding non-technology aspects of ethical hacking such as legal frameworks, documentation and report writing
Course Outcomes	:	After learning the course the students will be able to:
	CO1	Explain the importance of ethical hacking in achieving the goals of information security
	CO2	Differentiate the processes of vulnerability assessment and ethical hacking from penetration testing
	CO3	Comprehend the importance of appropriate countermeasures for managing vulnerabilities
	CO4	Justify the need for meticulous documentation in writing reports for consumption of both technical and management audiences
	CO5	Articulate the rationale for having an adequate legal framework for dealing with hacking and ethical hacking

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 of Assignments/Seminars/Presentations /MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**Introduction to Ethical Hacking:** Hacking Methodology, Process of Malicious Hacking, and Foot printing and scanning: Foot printing, scanning. Enumeration: Enumeration. System Hacking and Trojans: System Hacking, Trojans and Black Box Vs. White Box Techniques	07	20%	CO1
2	**Hacking Methodology:** Denial of Service, Sniffers, Session Hijacking and Hacking Web Servers: Session Hijacking, Hacking Web Servers. Web Application Vulnerabilities and Web Techniques Based Password Cracking: Web Application Vulnerabilities, Web Based Password Cracking Techniques	07	20%	CO2 CO3
3	**Web and Network Hacking:** SQL Injection, Hacking Wireless Networking, Viruses, Worms and Physical Security: Viruses and Worms, Physical Security. Linux Hacking: Linux Hacking. Evading IDS and Firewalls: Evading IDS and Firewalls	07	20%	CO1 CO4
4	**Report writing & Mitigation:** Introduction to Report Writing & Mitigation, requirements for low level reporting & high level reporting of Penetration testing results, Demonstration of vulnerabilities and Mitigation of issues identified including tracking	07	20%	CO2
5	**Ethical Hacking and Legal System:** Overview of India's Information Technology Amendment Act 2008 (IT Act 2008), hacker vs cracker, liabilities – civil and penal, cyber theft and IPC sec 378, IT Act 2008 – sections 43, 65 and 66, how to file a complaint of suspected hacking, Case Studies, understanding how hacking is legally dealt with among BRICS countries	08	20%	CO5

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.

Suggested List of Experiments/Tutorials

Sr. No.	Name of Experiment/Tutorial	Teaching Hours
1	Perform network scan to revile active hosts, open ports and services running.	01
2	Perform privilege escalation attack on Client operating system and gain control of a Client operating system and write a short note on its mitigation strategy.	01
3	Demonstrate ARP Poisoning and detect ARP Poisoning in switch-based network.	01
4	Perform man-in-the-middle attack and hijack an established session of a user. Write a report on the same with mitigation strategy.	02
5	Crack FTP credentials using dictionary attack and write a report of possible suggestion on hardening the login services.	01
6	Perform user system surveillance and write a mitigation report on the same.	02
7	Exploiting NetBIOS vulnerability and password revelation from browsers and social networking application using Key Logger and Trojan.	02
8	Perform denial service attack on a server operating system and write a report on the same with mitigation strategy.	02

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	VM Player; Windows server; Windows 7/ 10; Kali Linux; All-in-one keylogger; DELmE virus maker
2	I3/ I5 processor; 8GB RAM; 250GB HDD

Suggested Learning Websites

Sr. No.	Name of Website
1	https://www.javatpoint.com/ethical-hacking
2	https://www.udemy.com/topic/ethical-hacking/
3	https://www.youtube.com/watch?v=fNzpcB7ODxQ

Reference Books

Sr. No.	Name of Reference Books
1	The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson, Syngress; 2 edition (12 September 2013)
2	Hacking With Python: The Complete Guide to Ethical Hacking, Basic Security, Botnet Attack, Python hacking and Penetration Testing Kindle Edition by John C. Smalls
3	Hands-On Ethical Hacking and Network Defense by Michael T. Simpson | Kent Backman | James Corley, Cengage India 1st edition (2016)