Name of Faculty	:	**Faculty of Computer Science & Applications**
Name of Program	:	Master of Computer Application (MCA)
Course Code	:	2MCA06
Course Title	:	Cyber Security
Type of Course	:	Professional Core
Year of Introduction	:	2023-24

Prerequisite	:	Computer Network
Course Objective	:	Understand the web vulnerability, learn the network defence tools, and Cyber Law and it's application
Course Outcomes	:	At the end of this course, students will be able to:
	CO 1	Describe system and web vulnerability
	CO 2	Evaluate network defence tools
	CO 3	Understand the cyber laws
	CO 4	Investigate a cybercrime, prepare report and apply laws for the case

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	
2	0	4	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	**Systems Vulnerability Scanning:** Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection	8	25%	CO1

	tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet			
2	**Network Defense Tools Firewalls and Packet Filters:** Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Introduction Detection System	6	20%	CO2
3	**Web Application Tools Scanning for web vulnerabilities analysis tools:** Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap. DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra	6	20%	CO2
4	**Introduction to Cyber Crime and law Cyber Crimes and Digital Forensics:** Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Realms of the Cyber world, Recognizing and Defining Computer Crime, Contemporary Crimes, Contaminants and Destruction of Data, Indian IT ACT 2000	5	20%	CO3
5	**Introduction to Cyber Crime Investigation and Malware:** Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless Networks.	5	15%	CO4

Suggested List of Experiments/Tutorials

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

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	Which tool is the best for finding cyber attack/vulnerability.	04
2	Evaluate network defence tools for following:	04
3	IP spoofing	04
4	DOS attack	04
5	Explore the Nmap tool and list how it can be used for network defence.	04
6	Explore the NetCat tool.	04
7	Use Wireshark tool and explore the packet format and content at each OSI layer.	06
8	Examine SQL injection attack.	06
9	Perform SQL injection with SQLMap on vulnerable website found using google dorks.	06
10	Examine software keyloggers and hardware keyloggers.	06
11	Perform online attacks and offline attacks of password cracking.	06
12	Consider a case study of cybercrime, where the attacker has performed online credit card fraud. Prepare a report and list the laws that will be implemented on attacker.	06

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	Nmap Tool
2	NetCat Tool
3	Kali Linux OS
4	VMWare
5	DVWA Tool
6	PYCHARM

Suggested Learning Websites

Sr. No.	Name of Website
1	www.wireshark.org
2	https://hackaday.com/
3	https://breakthesecurity.cysecurity.org/
4	https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
5	https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
6	https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Reference books:

Sr. No.	Name of Reference Books
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley
2	Cyber Security and Cyber Laws Paperback – 2018 by Alfred Basta, Nadine Basta , Mary Brown , Ravinder Kumar, publication Cengage
3	Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
4	Cyber security and laws – An Introduction, Madhumita Chaterjee, Sangita Chaudhary, Gaurav Sharma, Staredu Solutions