B.M.S. COLLEGE OF ENGINEERING, BENGALURU-19

Autonomous Institute, Affiliated to VTU

DEPARTMENT OF CSE (IoT & Cyber Security including Blockchain)

Semester	**V**		
Course Title:	**Cyber Security**		
Course Code:	**23IC5PCCSY**	**Total Contact Hours: 40 hours**	
L-T-P:	**3-0-1**	**Total Credits:**	**4**

Unit No.	Topics	Hours
1	**Introduction to Cyber Security:** Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defense, Security Models, risk management, Cyber Threats- Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.	**8**
2	**Cyber crime**: **Mobile and Wireless Devices-** Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.	**8**
3	**Tools and Methods Used in Cyber crime:** Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. **Phishing and Identity Theft:** Introduction, Phishing, Identity Theft (ID Theft).	**8**
4	**Understanding Computer Forensics:** Introduction, Historical Background of Cyber Forensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation,	**8**

	Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Anti Forensics.	
5	**Cybersecurity- Organizational Implications:** Introduction, Cost of Cybercrimes and IPR issues, Web Threats for organizations, Security and Privacy implications from Cloud Computing, Social Media marketing, Social Computing and the Associated Challenges for Organizations, Organizational guidelines, Incident Handling, **Cybersecurity Standards and Frameworks:** DFARS, ISO 22301, HIPAA, NIST CSF **Cybercrime and Cyberterrorism:** Intellectual Property in the Cyberspace, The Ethical Dimension of Cybercrimes, The Psychology, Mindset and Skills of Hackers and Cybercriminal, Sociology of Cybercriminals, Information warfare.	**8**

Prescribed Text Book

Sl. No.	Book Title	Authors	Edition	Publisher	Year
1.	Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives	Sunit Belapure and Nina Godbole	1st	WILEY INDIA, .	2013
2.	Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives	B. B. Gupta, D. P. Agrawal, Haoxiang Wang	1st	CBS PUBLISHERS & DISTRIBUTORS PVT. LTD	2018

Reference Text Book					
Sl. No.	**Book Title**	**Authors**	**Edition**	**Publisher**	**Year**
1.	Cyber SecurityEssentials,	James Graham, Richard Howard and Ryan Otson,	1st	CRC Press.	2010
2.	Introduction to Cyber Security	Chwan-Hwa(john) Wu,J.David Irwin.	1st	CRC Press.	2013

E-Book						
Sl. No.	**Book Title**	**Authors**	**Edition**	**Publisher**	**Year**	**URL**
1.	CyBOK: The Cyber Security Body of Knowledge	Awais Rashid,Howard Chivers ,George Danezis, Emil Lupu, Andrew Martin -	1st	University of Bristol	2019	https://www.cybok.org/knowledgebase/
2.	Cybersecurity: The Beginner's Guide	Dr. Erdal Ozkaya	1st	Packt Publishing Ltd.	2019	https://www.jre-training.com/WebSecurity/Cybersecurity.pdf
3.	CyberSecurity for beginners	Heimdal Security team	-	heimdalsecurity	2011	https://heimdalsecurity.com/pdf/cyber_security_for_beginners_ebook.pdf

MOOC Course				
Sl. No.	**Course name**	**Course Offered By**	**Year**	**URL**
1.	Cyber Security	Swayam	2020	https://onlinecourses.swayam2.ac.in/cec20_cs15/preview
2.	Cyber Security and Privacy NPTEL	Swayam	2023	https://onlinecourses.nptel.ac.in/noc23_cs127/preview
3.	Introduction to Cyber Security	Swayam		https://onlinecourses.swayam2.ac.in/nou19_cs08/preview

Course Outcomes

At the end of the course, the student will be able to

CO1	Apply the concepts of cyber security, and cyber-crime.
CO2	Analyze threats and risks within the context of cyber security.
CO3	Design applications for cybercrime using appropriate cyber security methods.
CO4	Conduct experiments to implement cyber attacks and its countermeasures.

CO-PO mapping

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**
CO1	3							2					2		
CO2		3													
CO3			3		3			2							3
CO4				2	3										3

Proposed Assessment Plan (for 50 marks of CIE)

Assessment Tool	**No. of Assessments**	**Marks**
Internals	2	20
QUIZ	1	05
Lab	CIE + 1 Test	25
Total		**50**

B.M.S. COLLEGE OF ENGINEERING, BENGALURU-19

Autonomous Institute, Affiliated to VTU

DEPARTMENT OF CSE (IoT & Cyber Security including Blockchain)

SEE Exam Question paper format

Unit-1	Internal Choice	Two Question to be asked for 20 Marks each
Unit-2	Internal Choice	Two Question to be asked for 20 Marks each
Unit-3	Mandatory	One Question to be asked for 20 Marks
Unit-4	Mandatory	One Question to be asked for 20 Marks
Unit-5	Mandatory	One Question to be asked for 20 Marks

LAB EXPERIMENTS	
Experiment No.	**Name of the Experiment**
1	Installing and Configuring Kali Linux. Write a step-by-step guide to install Kali Linux on a virtual machine or a physical machine. This guide should cover the entire installation process, from downloading the ISO image to completing the installation and setting up the environment
2	Configure a firewall using iptables on a Linux system, write rules to filter traffic, and test its effectiveness against various network attacks.
3	Perform a network vulnerability scan using tools like Nessus or OpenVAS. Analyze the scan results to identify and prioritize vulnerabilities for remediation.
4	Develop and configure a simple Intrusion Detection System using Snort/WireShark to monitor network traffic and detect potential security breaches.
5	Capture and analyze network traffic for a simulated Advanced Persistent Threat (APT). Reconstruct the attack timeline using network forensic tools like Wireshark, NetworkMiner, Snort.
6	Simulate a Distributed Denial of Service (DDoS) attack in a controlled environment using LOIC/Slowloris, and analyze its impact on network performance.
7	Develop a custom keylogger in Python to capture keyboard inputs, and discuss ethical implications and countermeasures to detect such tools.
8	Analyze a malware sample in a controlled environment using Cuckoo Sandbox/ WireShark, identify its behavior, and suggest mitigation strategies.

9	Write a script to automate the process of scanning for IoT devices on a network using Shodan, identify vulnerabilities, and suggest security enhancements.