FACULTY OF ENGINEERING & TECHNOLOGY

Effective from Academic Batch: 2022-23

Programme: Bachelor of Technology (Artificial Intelligence (AI) & Data Science)

Semester: V

Course Code: 202045607

Course Title: Cyber Security

Course Group: Professional Elective Course – I

Course Objectives: This course provides the basis for understanding the fundamental issues surrounding the protection of information assets. The course's goal is to give students an overview of the topic of cyber security and assurance. Cyber Security is an area of study that investigates the possibilities of safe internet activity and how to safeguard oneself and, eventually, society against such attacks.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
3	0	2	4	50 / 18	50 / 17	25 / 09	25 / 09	150 / 53

* **J**: Jury; **V**: Viva; **P**: Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Introduction:** Introduction to Cyber Security, Importance and challenges in Cyber Security, Cyberspace, and Cyber threats, Cyber warfare, CIA Triad, Cyber Terrorism, Cyber Security of Critical Infrastructure, Cyber security -Organizational Implications.	06
2	**Hackers And Cyber Crimes:** Types of Hackers, Hackers and Crackers, Cyber-Attacks and Vulnerabilities, Malware threats, Sniffing, Gaining Access, Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks, Worms, Trojans, Viruses – Backdoors.	06
3	**Fundamentals of Ethical hacking and social engineering:** Ethical Hacking Concepts and Scopes - phases of ethical hacking, Enterprise Information Security Architecture, Vulnerability Assessment and Penetration Testing - Types of Social Engineering, Scanning and enumeration, Insider Attack, Preventing Insider Threats - Social Engineering Targets and Defense Strategies. Virtual LAN.	10
4	**Network Defense and Countermeasures:** Automated Security Assessment Tools (OpenVAS, Nessus), IDS, Honeypots and Firewalls, Cryptographic Attacks and Defenses. Password Cracking and Brute-Force Tools – John the Ripper, Pwdump, Firewalls and Packet Filters, VPN.	08

5	**Web Application Vulnerabilities:** Owasp Top 10 web application security, Application Inspection tools – Zed Attack Proxy, Sqlmap, DVWA.	**06**
6	**Introduction about Cyber Crime and Cyber Security:** Classification of cybercrimes and its examples, The legal perspectives, Cybercrime and the Indian ITA 2000, Global Perspective on Cybercrimes.	**04**
	Total	**40**

List of Practical's / Tutorials:

1	Introduction Virtualization Environment configuration and Cyber Lab setup (Kali, VM ware and Oracle VirtulBox).
2	Information Gathering using NMAP framework and study about port scanning.
3	Understand packet capturing tool wireshark or Ethercap and analysis of those packets.
4	Using open port information perform MITM (Man in the Middle) attack using arpspoof, urlsnarf, dsniff, dnsspoof. 1. Interruption 2. Interception
5	Understand the concept of firewall and configure the Statefull Packet Inspection (SPI) firewall IPTABLES.
6	BASIC configuration of Intrusion Detection System: Snort.
7	Network vulnerability assessment using OpenVAS/Necuss Framework.
8	Demonstrate automated SQL injection with SqLMap.
9	Demonstrate Application Injection using Zed Attack Proxy.
10	Perform web application testing using DVWA . 1. Perform Manual SQL injection 2. XSS using DVWA
11	Perform brute force attack using John the RIPPER.

Reference Books:

1	Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition.
2	Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
3	Cyber Security- Understanding Cyber Crimes, Computer Forensics and Legal Perspective", by Nina Godbole, Sunit Belapure, Wiley Publication.

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks						**R**: Remembering; **U**: Understanding; **A**: Application, **N**: Analyze; **E**: Evaluate; **C**: Create
R	**U**	**A**	**N**	**E**	**C**	
20%	25%	15%	10%	20%	10%	

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

Course Outcomes (CO):

Sr.	**Course Outcome Statements**	**% Weightage**
CO-1	Students will be able to explore various types of cyber-attacks.	**25**
CO-2	Capable of analyzing and evaluating penetration testing and vulnerability assessment techniques.	**25**
CO-3	To assure protection from the outside world, evaluate and secure Network and IT systems.	**25**

CO-4	Students will be able to acquire knowledge of types of cybercrimes, cyber laws and how to protect themselves.	**25**

Curriculum Revision:

Version:	2.0
Drafted on (Month-Year):	June-2022
Last Reviewed on (Month-Year):	-
Next Review on (Month-Year):	June-2025