COURSE CONTENT

CYBER SECURITY

V Semester: CSE

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
24X0520	Professional Elective I	2	0	2	3	40	60	100
Contact Classes: 48	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 48		

Prerequisites: Software Engineering

Course Overview:

The course offers a specialized undergraduate program that focuses on equipping students with the knowledge and skills to protect computer systems, networks, and data from cyber threats. The curriculum integrates core computer science engineering principles with specialized cybersecurity topics, preparing graduates for roles in ethical hacking, digital forensics, network security, and more.

Course Objectives:

The students will try to learn

1. Understand the fundamental concepts of cyber security, cybercrimes and cyber laws.
2. Apply cyber security operations, security concepts, preventions on the data.
3. Analyze and implement information gathering and security issues.
4. Design preventions on cyber-attacks and tools for mitigating them.
5. Utilize cyber security operations and learn how to detect a cyberattack.

Course Outcomes: After Completion of the Course, Students should be able to

1. Students be able to Explain the basics of cyber security, cybercrime and cyber law
2. Classify various types of attacks and learn the tools to launch the attacks
3. Apply various tools to perform information gathering
4. Apply intrusion techniques to detect intrusion
5. Apply intrusion prevention techniques to prevent intrusion

UNIT - I: Introduction: -

Cyber Security – History of Internet – Impact of Internet – CIA Triad; Reason for Cyber Crime – Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment. [10]

UNIT - II: Attacks and counter measure: -

OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures. [9]

UNIT - III: Reconnaissance: -
Harvester – Who is – Net craft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – Port Scanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches – SYN – Stealth – XMAS – NULL – IDLE – FIN Scans – Banner Grabbing and OS Finger printing Techniques. [9]

UNIT - IV: **Intrusion Detection: -**
Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed or Hybrid Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort. [10]

UNIT - V: Intrusion Prevention: -
Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations – Intrusion Prevention Systems – Example Unified Threat Management Products. [10]

TEXT BOOKS:

1. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021 (Unit 1)
2. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publishers, 2011 (Unit 1)
3. https://owasp.org/www-project-top-ten/

REFERENCE BOOKS:

1. David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", Jones & Bartlett Learning Publishers, 2013 (Unit 2)
2. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy", Elsevier, 2011 (Unit 3)
3. Kimberly Graves, "CEH Official Certified Ethical hacker Review Guide", Wiley Publishers, 2007 (Unit 3)
4. William Stallings, Lawrie Brown, "Computer Security Principles and Practice", Third Edition, Pearson Education, 2015 (Units 4 and 5)
5. Georgia Weidman, "Penetration Testing: A Hands-On Introduction to Hacking", No Starch Press, 2014 (Lab)

ELECTRONIC RESOURCES:

1) https://www.geeksforgeeks.org/cyber-security-tutorial/
2) https://www.tutorialspoint.com/cyber_security/index.htm
3) https://owasp.org/www-project-top-ten/
4) https://www.javatpoint.com/cyber-security-tutorial
5) https://www.cloudflare.com/learning/security/

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)