K. S. INSTITUTE OF TECHNOLOGY

An Autonomous Institution under VTU, Approved by AICTE

Department of Computer Science and Engineering

FIRST / SECOND SEMESTER SYLLABUS

Course : Introduction to Cyber Security		Semester	I/II
Course Code	**25BESC104H/ 204H**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40 Hours	Total Marks	100
Credits	03	Exam Hours	03
Examination type (SEE)	**Theory**		

Course objectives

- To familiarize cybercrime terminologies and perspectives
- To understand Cyber Offenses and Botnets
- To gain knowledge on tools and methods used in cybercrimes
- To understand phishing and computer forensics

Module-1

Introduction to Cybercrime:

Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global Perspectives

Textbook:1 Chapter 1 (1.1 to 1.5, 1.7-1.9)

Number of Hours: 08

Module-2

Cyber Offenses:

How Criminals Plan Them: Introduction, how criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercafé & cybercrimes.

Botnets: The fuel for cybercrime, Attack Vector. Textbook:1 Chapter 2 (2.1 to 2.7)

Number of Hours: 08

Module-3

Tools and Methods used in Cybercrime: Introduction, Proxy Servers, Anonymizers, Phishing, Password Cracking, Key Loggers and Spy ways, Virus and Worms, Trozen Horses and Backdoors, Steganography, DoS and DDOS Attacks, Attacks on Wireless networks.

Textbook:1 Chapter 4 (4.1 to 4.9, 4.12)

Number of Hours:08

Module-4

Phishing and Identity Theft: Introduction, methods of phishing, phishing, phishing techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft

Textbook:1 Chapter 5 (5.1. to 5.3) Number of Hours: 08

Module-5

Understanding Computer Forensics: Introduction, Historical Background of Cyber forensics, Digital Forensics Science, Need for Computer Forensics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics.

Textbook:1 Chapter 7 (7.1. to 7.5, 7.7 to 7.9) Number of Hours: 08

Suggested Learning Resources

Textbooks:

Sunit Belapure and Nina Godbole,"CyberSecurity: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, 2011, First Edition (Reprinted 2018

Course outcome (Course Skill Set)

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

CO1: Define and explain key terminologies related to cybercrime.
CO2: Describe Cyber offenses and Botnets
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Explain the concepts of phishing and identity theft with relevant examples.
CO5: Describe the need of computer forensics in investigating and preventing cybercrime.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=nzZkKoREEGo&list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_
- https://www.youtube.com/watch?v=6wi5DI6du-4&list=PL_uaeekrhGzJlB8XQBxU3zhDwT95xlk
- https://www.youtube.com/watch?v=KqSqyKwVuA8

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Illustration of standard case study of cyber crime
- Setup a cyber-court at Institute level

Assessment Structure:

The assessment in each course is divided equally between Continuous Internal Evaluation (CIE) and the Semester End Examination (SEE), with each carrying 50% weightage.

- To qualify and become eligible to appear for SEE, in the **CIE**, a student must score at least **40% of 50 marks**, i.e., **20 marks**.
- To pass the **SEE**, a student must score at least **35% of 50 marks**, i.e., **18 marks**.

Not- withstanding the above, a student is considered to have **passed the course,** provided the combined total of **CIE and SEE is at least 40 out of 100 marks**.

Continuous Comprehensive Assessments (CCA):

CCA will be conducted for a total of 25 marks. It is recommended to include a maximum of two learning activities aimed at enhancing the holistic development of students. These activities should align with course objectives and promote higher-order thinking and application-based learning.

Learning Activity -1: **Marks- 15**

Learning Activity -2 : **Marks-10**