26.10.2022

Course Title:	Introduction to Cyber Security		
Course Code:	**22ETC154/254**	CIE Marks	50
Course Type (Theory/Practical /Integrated)	Theory	SEE Marks	50
		Total Marks	100
Teaching Hours/Week (L:T:P: S)	3-0-0-0	Exam Hours	03
Total Hours of Pedagogy	40 hours	Credits	03

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

Teaching-Learning Process

These are sample Strategies, which teacher can use to accelerate the attainment of the various course outcomes and make Teaching –Learning more effective

1. Chalk and Board
2. Demonstration
3. Interactive learning
4. Videos and online material

Module-1 (8 hours of pedagogy)

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)

Module-2 (8 hours of pedagogy)

Cyber Offenses:

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

Botnets: The fuel for cybercrime, Attack Vector.

Textbook:1 Chapter 2 (2.1 to 2.7)

Module-3 (8 hours of pedagogy)

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

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

Module-4 (8 ours of pedagogy)

Phishing and Identity Theft: Introduction, methods of phishing, phishing,phising 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)

Module-5 (8 hours of pedagogy)

Understnading Computer Forensics: Introdcution, Historical Background of Cyberforensics, Digital Foresics Science, Need for Computer Foresics, 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)

Course outcome (Course Skill Set)

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

CO1	Explain the cybercrime terminologies
CO2	Describe Cyber offenses and Botnets
CO3	Illustrate Tools and Methods used on Cybercrime
CO4	Explain Phishing and Identity Theft
CO5	Justify the need of computer forensics

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50). The minimum passing mark for the SEE is 35% of the maximum marks (18 marks out of 50). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 35% (18 Marks out of 50) in the semester-end examination (SEE), and a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation(CIE):

Two Unit Tests each of 30 Marks (duration 01 hour)

- First test after the completion of 30-40 % of the syllabus
- Second test after completion of 80-90% of the syllabus

One Improvement test before the closing of the academic term may be conducted if necessary. However best two tests out of three shall be taken into consideration

Two assignments each of 20 Marks

The teacher has to plan the assignments and get them completed by the students well before the closing of the term so that marks entry in the examination portal shall be done in time. Formative (Successive) Assessments include Assignments/Quizzes/Seminars/ Course projects/Field surveys/ Case studies/ Hands-on practice (experiments)/Group Discussions/ others. . The Teachers shall choose the types of assignments depending on the requirement of the course and plan to attain the Cos and POs. (to have a less stressed CIE, the portion of the syllabus should not be common /repeated for any of the methods of the CIE. Each method of CIE should have a different syllabus portion of the course). CIE methods /test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

The sum of two tests, two assignments, will be out of 100 marks and will be scaled down to 50 marks

Semester End Examination(SEE):

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the subject (**duration 03 hours)**

- The question paper shall be set for 100 marks. The medium of the question paper shall be English/Kannada). The duration of SEE is 03 hours.
- The question paper will have 10 questions. Two questions per module. Each question is set for 20 marks. The students have to answer 5 full questions, selecting one full question from each module. The student has to answer for 100 marks and **marks scored out of 100 shall be proportionally reduced to 50 marks**.
- There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.

Suggested Learning Resources:

Books (Title of the Book/Name of the author/Name of the publisher/Edition and Year)

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

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=yC_hFm0BX28&list=PLxApjaSnQGi6Jm7LLSxvmNQjS_rt9swsu
- https://www.youtube.com/watch?v=nzZkKoREEGo&list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_
- https://www.youtube.com/watch?v=6wi5DI6du-4&list=PL_uaeekrhGzJlB8XQBxU3z__hDwT95xlk
- 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

COs and POs Mapping (Individual teacher has to fill up)

COs	POs											
	1	2	3	4	5	6	7	8	9	10	11	12
CO1												
CO2												
CO3												
CO4												
CO5												

Level 3- Highly Mapped, Level 2-Moderately Mapped, Level 1-Low Mapped, Level 0- Not Mapped