Course: BTech　　　　　　　　　　　　　　　　　　　　　　　　　　　　**Semester:** 1

Prerequisite: Basic knowledge of networking.

- **Rationale:** Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
0	0	2	0	1	-	-	30	-	20	50

SEE - Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Outcome

After Learning the Course, the students shall be able to:

1. Reasonable understanding of the fundamentals of the cybersecurity domain and related issues

2. Practical knowledge of various tools, processes and methods to ensure security of systems through a minimum of two hands-on assignments involving attack and protection in a virtual environment

3. An understanding of the inter-disciplinary nature of cybersecurity domain

4. Adequate level of cross-disciplinary knowledge of design, implementation, evaluation and testing of secure protocols, systems or applications

5. Basic knowledge to be able to build bug-free systems, dependable during malice or error
6. Foundational skills for developing expertise in one or more sub-domains of cyber-security

List of Practical	
1.	**Practical-1** Use of hashes to check the integrity of the file.
2.	**Practical-2** Perform passive information gathering techniques to gather the information of the target.
3.	**Practical-3** Perform active information gathering techniques to gather the information of the target.
4.	**Practical-4** Perform Basic Linux commands for file handling.
5.	**Practical-5** Set-up OSINT framework tool on windows. (Spiderfoot)
6.	**Practical-6** Setting up IdAM in windows server
7.	**Practical-7** Perform vulnerability scanning using nmap
8.	**Practical-8** CASE STUDY on UPI Security.
9.	**Practical-9** Implementation of MITM- attack using wireshark / network sniffers.
10.	**Practical-10** Implementation of Steganography.