

Course Code	Course Title	L	T	P	C
BCSE410L	Cyber Security	3	0	0	3
Pre-requisite	NIL	Syllabus version			
		1.0			
Course Objectives					
1. To understand the need for cybersecurity for solving the real word problems					
2. To aware of ethical hacking methodologies for protecting cyber-physical systems.					
3. To familiarize the defensive mechanisms, countermeasures, and best practices.					
Course Outcomes					
1. Understand the emerging cybersecurity attacks and their adversarial risk					
2. Identify the emerging vulnerabilities and attacks, and countermeasures in cyber-physical systems.					
3. Comprehend the need for ethical hacking to minimize the security risk					
4. Know the emerging security solutions using automated tools and techniques					
Module:1 Foundation for Cyber Security 4 hours					
Hacker - Ethical hacker - Cyber-attacks: Network infrastructure attacks, Operating system attacks, Application and other specialized attacks - Security Assessment Principles					
Module:2 Hacking Methodology 5 hours					
Methodology: Scanning the Systems and Network - Attack tree analysis - Assessing Vulnerabilities - Penetration Testing - Security Testing tools					
Module:3 Social Engineering 7 hours					
Social Engineering Implications - Performing Social Engineering Attacks - Social Engineering Countermeasures: Policies, User awareness and training - Social Engineering Tool kit - Physical Security					
Module:4 Password Security 7 hours					
Password Vulnerabilities - Passwords Cracking Tools - Brute-force attacks - Rainbow attack - Password Cracking Countermeasures - Password Policy - Securing Operating Systems - Keyloggers tools					
Module:5 Wireless and Mobile Security 7 hours					
Wireless and mobile Vulnerabilities and Attacks - Encrypted Traffic and countermeasures - Rogue wireless devices and countermeasures - MAC spoofing and countermeasures - Securing wireless workstations, Wi-Fi and Internet of Things					
Module:6 Operating System Security 6 hours					
OS Vulnerabilities: Windows, Linux and Mac - Detecting Null Sessions - Exploiting Missing Patches – Metasploit - Burp suite - Countermeasures against Buffer overflow and NFS attacks					
Module:7 Web Application and Databases Security 7 hours					
Web App Security: Seeking out Web Vulnerabilities - Directory traversal - Input-filtering attacks - Code injection, SQL injection, Cross-site scripting Counter					

measures - Database Security: Database vulnerabilities - Minimizing Database Security Risks and Storage Security Risks – Counter measures and tools			
Module:8		Recent Trends	
		2 hours	
Guest lectures from Industry and, Research and Development Organizations			
		Total Lecture hours:	
		45 hours	
Text Book(s)			
1.	Kevin Beaver CISSP, Hacking for Dummies, 2022, John Wiley & Sons, Inc, 7th Edition		
Reference Books			
1.	Nina Godbole, SunitBelapure, Cyber Security, Understanding cybercrimes, computer forensics and legal perspectives, Reprint 2016, Wiley Publications		
2	Brooks, Charles J., Christopher Grow, Philip Craig, and Donald Short, Cybersecurity essentials, 2018, John Wiley & Sons,		
3.	Sammons, John, and Michael Cross. The basics of cyber safety: computer and mobile device safety made easy, 2016, Elsevier.		
4	Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies; Security in Computing, 2015, Pearson Education Inc., 5th Edition.		
Mode of Evaluation: CAT, Assignment, Quiz, FAT			
Recommended by Board of Studies		12-05-2023	
Approved by Academic Council		No. 70	Date 24-06-2023