Course Code	PCA20D02J	Course Name	CYBER SECURITY	Course Category	D	*Discipline Elective* Course	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Computer Applications		Data Book / Codes/Standards	Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to,	Learning

CLR-1 :	*Have an overview of cyber crime scenario and legal perspective on cyber crime.*
CLR-2 :	*Understand different types of cyber attacks*
CLR-3 :	*Understand about tools and methods used in cyber crime.*
CLR-4 :	*Understand the need of cyber laws*
CLR-5 :	*Understand and know how cyber forensics is used in cyber crime investigations*
CLR-6 :	*Create/ setup methodologies for understand and avoid becoming victims of cyber crime*

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	*Identify different classification of cybercrimes.*	*3*	*80*	*70*
CLO-2 :	*Apply the logic of Performing cyber forensics.*	*3*	*85*	*75*
CLO-3 :	*Analyze about the various kinds of vulnerabilities and scanning them.*	*3*	*75*	*70*
CLO-4 :	*Apply the various types of firewalls to effective ensure security of the premises*	*3*	*85*	*80*
CLO-5 :	*Identify and solve Web Treats for Organizations: The Evils and Perils*	*3*	*75*	*70*
CLO-6 :	*Apply tools and methods of cyber-crime concepts to solve security problems & Learn about providing Security solutions*	*3*	*85*	*80*

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research Skills	Team Work	Scientific Reasoning	Reflective Thinking	Self-Directed Learning	Multicultural Competence	Ethical Reasoning	Community Engagement	ICT Skills	Leadership Skills	Life Long Learning
L	*H*	*H*	*H*	*H*	*M*	-	*H*	*M*	*H*	-	*H*	*H*	-	*M*
M	*M*	*H*	*H*	*H*	-	-	*M*	*M*	*M*	-	*H*	*M*	-	*L*
M	*M*	*H*	*H*	*H*	-	-	*M*	*M*	*L*	-	*H*	*M*	-	*H*
L	*L*	*H*	*H*	*H*	*M*	-	*M*	*L*	*H*	*M*	*H*	*M*	-	-
H	*H*	*H*	*H*	*H*	*L*	-	*M*	*H*	*L*	*L*	*H*	-	*L*	-
L	*H*	*H*	*H*	*H*	*H*	-	*M*	*M*	*L*	*H*	*H*	-	*L*	-

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Cybercrime definition and origins	Proxy Servers- Anonymizers	The Legal Perspectives	Historical Background of Cyber forensics, Digital Forensics Science	Organizational Implications, Cost of Cybercrimes and IPR Issues ,
S-2	SLO-1	Cybercrime and information security	Phishing- Password Cracking	Need of Cyberlaw:	The Need for Computer Forensics- Cyber forensics and Digital Evidence	Lesson for Organizations, Web Treats for Organizations:
S-3	SLO-1	Classifications of cyber crime-	Keyloggers and Spywares-	The Indian Context	Forensics Analysis of Email, Digital Forensics Lifecycle	The Evils and Perils, Security and Privacy Implications from Cloud Computing
S-4-5	**SLO-1**	**Lab 1: Cyber security attacks-case study Submission**	**Lab 4: TCP / UDP connectivity using Netcat**	**Lab 7 : Demonstrate how to provide secure data storage,**	**Lab 10: Perform an experiment how to use dumpsec**	**Lab 13:Setup a honey pot on network.**

				secure data transmission and for creating digital signatures (GnuPG)		
S-6	SLO-1	Cybercrime and the Indian ITA 2000	Virus and Worms	The Indian IT Act	Chain of Custody Concept, Network Forensics	Social Media Marketing:Security Risk and Perils for Organization
S-7	SLO-1	A global Perspective on cybercrimes	Steganography	Digital Signature and the Indian IT Act	Approaching a Computer Forensics Investigation	Social Computing and the Associated Challenges for Organizations
S-8	SLO-1	How criminal plan the attacks	DoS -DDoS Attacks	Amendments to the Indian IT Act	Computer Forensics and Steganography	Protecting People's Privacy in the Organization
S-9 to S-10	**SLO-1**	**Lab 2: Cyber security attacks-case study Submission**	**Lab 5: TCP / UDP connectivity using Netcat**	**Lab 8 : Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)**	**Lab 11: Perform an experiment how to use dumpsec**	**Lab 14: Monitor the honey pot on network.**
S-11	SLO-1	Social Engineering- Cyber stalking	SQL Injection, Buffer Over Flow	Cybercrime and Punishment	Relevance of the OSI 7 Layer Model to the Computer Forensics and Social Networking Sites	Organizational Guidelines for Internet Usage
S-12	SLO-1	Cybercafe- Cybercrimes- Botnets	Attacks on Wireless Networks, Phishing	Cyberlaw	The Security/Privacy Threats	Safe Computing Guidelines
S-13	SLO-1	Attack vector- Social Engineering-Cloud Computing	Identity Theft (ID Theft)	Technology and Students: Indian Scenario	Forensics Auditing, Anti Forensics	Computer Usage Policy Incident Handling
S-14 to S-15	**SLO-1**	**Lab 3: TCP scanning using NMAP Port scanning using NMAP**	**Lab 6: Perform an experiment to demonstrate sniffing of router traffic by using the tool Wireshark**	**Lab 9:Perform an experiment to sniff traffic using ARP Poisoning**	**Lab 12: Implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols**	**Lab 15: Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w)**

Learning Resources	1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and SunitBelpure, Publication Wiley	2. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication McGraw Hill. 3. Nina Godbole, Information Systems Security, Wiley India, New Delhi 4. Cyrus Piekari, Anton Chuvakin, "Security Warrior", 2nd ed., Oreilly Publishers, 2005.

Learning Assessment											
Level	Bloom's Level of Thinking	Continuous Learning Assessment (50% weightage)								Final Examination (50% weightage)	
		CLA – 1 (10%)		CLA – 2 (10%)		CLA – 3 (20%)		CLA – 4 (10%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember	20%	20%	15%	15%	15%	15%	15%	15%	20%	20%
	Understand										
Level 2	Apply	20%	20%	20%	20%	20%	20%	20%	20%	20%	20%
	Analyze										
Level 3	Evaluate	10%	10%	15%	15%	15%	15%	15%	15%	10%	10%
	Create										
	Total	100 %		100 %		100 %		100 %		100 %	

CLA – 4 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, Conf. Paper etc.,

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
Mr.G.Muruganandam, Group Project Manager, HCL Technologies, Chennai	*Dr.S.Gopinathan, Professor, University of Madras, Chennai*	*Mr.N.KRISHNAMOORTHY, SRMIST*
Mr.M. Hemachandar, Tech Lead, Wipro Limited, Chennai		