GUJARAT TECHNOLOGICAL UNIVERSITY

CYBER SECURITY (59)
CYBER CRIMES, ETHICS AND LAWS
SUBJECT CODE: 3715905
SEMESTER: I

Type of course: ME Cyber Security

Prerequisite: NA

Rationale: This course explores technical, legal, and social issues related to cybercrime. Cybercrime is a broad term that includes offences where a computer may be the target, crimes where a computer may be a tool used in the commission of an existing offence, and crimes where a computer may play a subsidiary role such as offering evidence for the commission of an offence. The origins and extent of cybercrime, responses from legal systems to cyber-criminals, and the social impact of cybercrimes will be addressed. Various types of cybercrimes, cyber-criminals, as well as the motivations and methods involved in cyber-offences will be explored. Human and intellectual issues and jurisdictional challenges will be critically examined.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Sr. No.	Content	Total Hrs	% Weightage
1	Cyber Crime : Definition and Origin of the Word, Cyber Crime and Information Security, Who are Cyber Criminals, Classification of Cyber crimes, E-mail Spoofing, Spam ming, Cyber Defamation, Internet Time Theft, Salami Attack, Salami technique Data Diddling, Frogery, Web Jacking,Newsgroup Spam, Industrial Spying,, Hacking, Online Fruads, Pornograpic Offenders, Software Piracy, Computer Sabotage Email Bombing, Computer Network Intruision, Password Sniffing, Credit Card Frauds, Identity Theft	6	15
2	Cyber Crime : The Legal Perspectives, The Cyber Crime Indian Perspectives, The Cyber Crime And Indian ITA 2000/2001, Hacking and Indian Laws, Global Perspective on Cyber Crime , Cyber Crime and extended Enterprise, Cyber Crime Era : Survival Mantra for Netizens	4	10

3	Cyber Offenses : How Criminals plan them, Categories of Cyber Crimes, How Criminal Plans the Attack : Active Attcks, Passive Attacks, , Social Engineering, Classification of Social Engineering, Cyber Stalking : types of Stalkers, Cyber Cafe and Cyber Crimes, Botnets , Attck Vectors, Cyber Crime and Cloud Computing	4	10
4	Cybercrime: Mobile and Wireless Devices, Proliferation of Mobile and Wireless devices, Trends in Mobility, Credit card Frauds in Mobile and wireless devices, Authentication Service Security, Attacks on Mobile/Cellphones, Mobile Devices: Security Implications for Organizations, Organization Security polices and Measures in Mobile Computing Era	5	10
5	Tools and Methods used in Cybercrime: Proxy server and Anonymizers, phising: How Phishing works? How password cracking works? Keylogers and Spywares, Virus and Worms, Trozan Horses and Backoors, Dos and Ddos Attacks, SQL Injection, Buffer Overflow, An Attacks on Wireless Networks	5	10
6	Phishing and Identity Theft: Phishing: Methods of Phishing, Phishing Techniques, Types of Phishing Scams, Phishing countermeasures, Identity theft, Types and Techniques of identity thefts and its counter measures	4	5
7	Cybercrimes and Cybersecurity: The legal perspectives: Cybercrimes and the legal Landscape around the world, why do we need cyberlws: The indian context, The indian IT ACT: Admisibilty of Electronic records, Amendments made in Indian ITA 2000,Psitive Aspects and weak areas of ITA 2000, Chanllenges to indin law and cybercrime scenario in India, Digital signatures and the Indian ITA act, Cybercrime and punishment, Cyber law Technology and students: Indin Scenario	6	15
8	Understanding Computer Forensics: Digital forensic Science, Need for Computer Foransic, Cyber Forensic and digital Evidence and rules of Evidence, Forensics Analysis of E-Mail, Digital Forensic Life Cycle,	5	10
9	Cyber Security: Organizational Implications: Web Threats for Organization , Security and Privacy Implications, Social Media Marketing: Security risk for organizations, Incident handling: An Essential Component of Cyber Security, Intellectual Property in the Cyberspace, The Ethical Dimensions of Cybercrime, The Psycology, Mindset and skills of Hackers and the Other criminals	5	10
10	Cybercrime: Examples and Mini cases	4	5

Reference Books:

1. Cyber Security : Understanding Cyber Crimes , Computer Forensics and Legal Perspectives By Nina Godbole, Sunit Belapur , Wiley
2. UNDERSTANDING CYBERCRIME: P H E N O M E N A , A N D L E G A L C H A L L E N G E S R E S P O N S E, ITU 2012

Course Outcome:

After learning the course the students should be able to:

1. To identify and describe the major types of cyber crime.
2. To identify cyber crime vulnerabilities and exploitations of the Internet.
3. To identify the four major cyber crimes vulnerability areas:
   a. physical security, personal security, communications security, and operations security.
4. Distinguish between various types of cybercrimes with respect to the motivations and methods of operation of offenders, the types of victims or targets, and the spatial, temporal, and legal domains in which they are carried out.
5. Identify various classifications of cybercrimes and cyber-criminals.
6. To identify appropriate responses to cyber criminal activity.
7. To understand the law with regards to the investigation and prosecution of cyber criminals.
8. To identify appropriate law enforcement strategies to both prevent and control cyber crime.
9. Explain jurisdictional challenges that nations face when responding to cybercrime

List of Experiments:

1. Algorithm Buffer overflow attack.
2. Implementation of SQL injection so the query with attack parameters using SQL so the query with parameters.
3. Using cross scripting with Java script programming so the vulnerability in any of the web page.
4. Using a facebook API give a demonstration of defacement with embedding a fake photograph.
5. Using dynamic analysis analysis so the behavior with a vulnerability of any security program.
6. Analysis a java program using static analysis Disassembler tools.
7. Development tools for password cracking.
8. Implement algorithm treat identity theft.
9. Using flooding technique implement DDOS attack.
10. Implementation key loggers.