



GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering

Subject Code: 3163213

CYBER CRIME AND MITIGATION

6th SEMESTER

Type of course: Undergraduate (Elective)

Prerequisite: NA

Rationale: This course explores technical, legal, and social issues related to cybercrime. The origins and extent of cybercrime, responses from legal systems to cyber-criminals, and the social impact of cybercrimes will be addressed. The course explores implementation of firewalls for different operating systems and at different layers of network architecture. The course also explores mitigation at various stages of operating systems, network and endpoint.

Teaching and Examination Scheme:

Teaching Scheme			Credits C	Examination Marks				Total Marks
L	T	P		Theory Marks		Practical Marks		
			ESE (E)	PA (M)	ESE (V)	PA (I)		
3	0	0	3	70	30	0	0	100

Course Contents:

Sr. No	Content	Total Hrs.	Marks Weightage (%)
1	Cyber Crimes: Definition and Origin of the Word, Cyber Crime and Information Security, Who are Cyber Criminals, Classification of cyber crimes, E-mail Spoofing, Spamming, Forgery, Hacking, Online Fruads, Software Piracy, Computer Sabotage Email Bombing, Computer Network Intrusion, Password Sniffing, Credit Card Frauds, Phishing, vishing, Identity Theft, Social Engineering, CPU Hijackers, Darknets and Dark Markets.	9	20
2	Definition and Terminology (Information Technology Act, 2000): 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, Cybercrime and punishment, Cyber Crime Era : Survival Mantra for Netizens.	4	5
3	Firewalls: Windows Host based Firewall, Windows Firewall Control, Linux Host based Firewalls-iptables, UFW, gufw & nftables, Mac - Host based Firewalls - pflist, Icefloor & Murus, Little Snitch, Network based firewalls -Routers - DD-WRT,Hardware, pfSense, Smoothwall and Vyos.	8	15



GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering

Subject Code: 3163213

4	Operating System Security and Privacy: Security features and functionalities, Security bugs and vulnerabilities, OS Privacy and Tracking, General Use Operating Systems With a Security and Privacy Focus, Penetration Testing and Ethical Hacking Focused Operating Systems, Mobile Operating Systems with Security & Privacy Focus.	8	20
5	Network Security: Network Attacks and Network Isolation, Wi-Fi Weaknesses, Wi-Fi Security Testing-Secure Configuration and Network Isolation, Network Monitoring for threats, search engine and privacy , Browser Security Password and authentication methods	8	20
6	End Point Protection: File and Disk Encryption, Next Generation - Anti-Virus (NG-AV) & End-Point-Protection (NG-EPP), End Point Protection Technology, Threat Detection and Monitoring, Email- Security and Privacy Messengers - Security and Privacy.	8	20

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	25	15	10	5	5

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books:

1. Cyber Security : Understanding Cyber Crimes , Computer Forensics and Legal Perspectives By Nina Godbole, Sunit Belapur , Wiley
2. Understanding Cyber Crime: Phenomena and Legal Challenges Response, ITU 2012
3. Building Internet Firewalls: Internet and Web Security by Elizabeth D. Zwicky, Simon Cooper, , D. Brent Chapman, Addison -Wesley Professional Computing Series
4. Penetration Testing with Shellcode: Detect, exploit, and secure network-level and operating system vulnerabilities by Hamza Megahed ,Packt Publishing Publisher
5. Network Monitoring and Analysis: A Protocol Approach to Troubleshooting by Ed Wilson, Prentice Hall publisher (January 9, 2000)
6. Symantec Endpoint Protection Standard Requirements by Gerardus Blokdyk,5 STAR Cooks publisher



GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering

Subject Code: 3163213

Course Outcome:

After learning the course the students should be able to:

Sr. No.	CO Statement	Marks % Weightage
CO-1	To identify and describe the major types of cybercrime.	10
CO-2	To understand the law with regards to the investigation and prosecution of cyber criminals.	15
CO-3	To configure operating system security, privacy, and patching - On Windows, MacOS and Linux.	20
CO-4	To Configure firewalls on all platforms for all types of attack scenarios.	15
CO-5	To develop practical skill set in ensuring network security against all threats.	20
CO-6	To diversify technologies offered by end-point-protection software, from traditional approaches, through to next generation and future technology.	20