GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Post Graduate Diploma

Level: PG Diploma

Branch: Cyber Security

Subject Code : PI01001031

Subject Name : Cyber Security Techniques

w. e. f. Academic Year:	2025-26
Semester:	1
Category of the Course:	Core Course

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes
CO-1	**Analyze** advanced cyber threats, attack vectors, and modern security challenges.
CO-2	**Implement** security mechanisms for data protection, access control, and system hardening.
CO-3	**Apply** cryptographic and steganographic techniques for secure communication.
CO-4	**Evaluate** security measures for cloud computing, mobile applications, and IoT environments.
CO-5	**Perform** ethical hacking and penetration testing to identify vulnerabilities.
CO-6	**Develop** strategies for digital forensics, incident response, and cyber threat intelligence

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
4	0	2	5	70	30	20	30	150

Course Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	**Advanced Cyber Threats and Attack Techniques:** Modern Cyber Threats: APTs, Ransomware, Fileless Malware, Attack Vectors: Zero-day Exploits, Botnets, DDoS, Social Engineering and Phishing Techniques, MITRE ATT&CK Framework for Threat Analysis	6	10

2	**System and Application Security Hardening:** Secure System Configuration and Patch Management, Secure Boot, BIOS/UEFI Security, Application Sandboxing and Container Security (Docker, Kubernetes), Windows and Linux System Hardening Techniques.	**8**	**15**
3	**Cryptography and Steganography for Cyber Defense:** Advanced Cryptographic Techniques: Elliptic Curve Cryptography (ECC), Homomorphic Encryption, Blockchain Security and Smart Contracts, Quantum-Safe Cryptography, Data Hiding Techniques: Image and Audio Steganography	**8**	**15**
4	**Network and Cloud Security Techniques:** Advanced Firewall Techniques (Next-Gen Firewalls, UTM), Zero Trust Network Architecture (ZTNA), Secure Cloud Storage, Data Loss Prevention (DLP), Container Security in Cloud Computing	**8**	**15**
5	**Mobile and IoT Security:** Mobile App Security: Reverse Engineering, Secure App Development, Rooting, Jailbreaking, and Mobile Malware Analysis, IoT Security Challenges: Botnets, Secure Communication in IoT, Lightweight Encryption for IoT Devices	**06**	**10**
6	**Ethical Hacking and Red Team Operations:** Penetration Testing Methodologies, Exploitation Frameworks (Metasploit, Cobalt Strike), Web Application Security Testing (Burp Suite, SQLMap), Wireless Hacking Techniques (Wi-Fi Attacks, Bluetooth Exploits)	**08**	**20**

References/Suggested Learning Resources:

(a) Books:

1. **"Cryptography and Network Security: Principles and Practice"** – William Stallings
2. **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"** – Dafydd Stuttard, Marcus Pinto
3. **"Hacking: The Art of Exploitation"** – Jon Erickson
4. **"Computer Forensics and Cyber Crime: An Introduction"** – Marjie T. Britz.

List of open Source software/learning Websites:

- Kali Linux – A penetration testing and ethical hacking Linux

distribution. (https://www.kali.org/)

- OWASP ZAP – Open-source web application security scanner. (https://owasp.org/www- project-zap/)
- Metasploit Framework – Exploitation framework for penetration testing. (https://www.metasploit.com/)
- Cybrary – Free cybersecurity courses and certification resources. (https://www.cybrary.it/)
- TryHackMe – Interactive cybersecurity training platform. (https://tryhackme.com/)

* * * * * * *