



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Post Graduate Diploma

Level: PG Diploma

Branch: Cyber Security

Subject Code : PI01001011

Subject Name : Principles of Cyber Security

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	Identify cybersecurity risks, threats, and attack vectors.
CO-2	Analyze attack mechanisms and system vulnerabilities.
CO-3	Apply cryptographic and network security techniques.
CO-4	Evaluate security solutions in cloud and network environments
CO-5	Interpret cybersecurity policies, governance, and risk management principles

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
L	T	PR	C	Theory		Tutorial / Practical		
				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	Introduction to Cyber Security: Overview and Importance, Cybersecurity vs. Information Security, CIA Triad: Confidentiality, Integrity, Availability, Threats, Vulnerabilities, and Attack Vectors, Security Policies and Frameworks (NIST, ISO 27001)	5	6



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Post Graduate Diploma

Level: PG Diploma

Branch: Cyber Security

Subject Code : PI01001011

Subject Name : Principles of Cyber Security

2	Cyber Threats and Attacks: Types of Cyber Attacks: Malware, Phishing, DoS/DDoS, Ransomware, Advanced Persistent Threats (APT), Social Engineering Attacks, Attack Life Cycle and Kill Chain, Case Studies on Major Attacks.	8	14
3	Cryptography and Security Mechanisms: Basics of Cryptography, Symmetric vs. Asymmetric Encryption (AES, DES, RSA, ECC), Hashing (SHA, MD5) and Digital Signatures, Public Key Infrastructure (PKI) and Certificates, Cryptographic Protocols: SSL/TLS, IPSec	9	16
4	Network Security: Network Protocols and Security Issues, Firewalls, IDS, IPS, and VPNs, Wireless Network Security (Wi-Fi, Bluetooth), Web Security: HTTPS, SSL/TLS, Secure Network Design and Zero Trust Model	12	22
5	System and Application Security: Secure Software Development Life Cycle (SDLC), Web Application Security (OWASP Top 10), Operating System Security (Windows, Linux, Android), Secure Coding Practices, Security Hardening Techniques	08	14
6	Cyber Laws, Ethics, and Compliance: Cybercrime and Legal Frameworks (IT Act, GDPR, HIPAA, PCI-DSS), Intellectual Property Rights (IPR) and Cyber Ethics, Incident Response and Digital Forensics	07	13

References/Suggested Learning Resources:

(a) Books:

1. Principles of Computer Security: CompTIA Security+ and Beyond by Wm. Arthur Conklin, Gregory White | McGraw-Hill
2. Cryptography and Network Security: Principles and Practice by William Stallings | Pearson
3. The Web Application Hacker's Handbook by Dafydd Stuttard, Marcus Pinto | Wiley
4. Network Security Essentials: Applications and Standards by William Stallings | Pearson.
5. Computer Forensics and Cyber Crime: An Introduction by Marjie T. Britz | Pearson.

List of Experiments

- 1) Install and configure **VirtualBox/VMware** and Set up **Kali Linux and Windows/Linux test environments** for cybersecurity experiments.
- 2) Implement **AES (Advanced Encryption Standard) and RSA encryption** using Python or OpenSSL.



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Post Graduate Diploma

Level: PG Diploma

Branch: Cyber Security

Subject Code : PI01001011

Subject Name : Principles of Cyber Security

- 3) Generate **SHA-256 and MD5 hashes** for files and passwords.
- 4) Use **Nmap** to scan a network for open ports and services and Identify vulnerabilities and active hosts in a network.
- 5) Set up and configure **iptables (Linux) or Windows Firewall** and Block/unblock specific ports and test firewall rules.
- 6) Perform **SQL Injection and XSS attacks** using DVWA (Damn Vulnerable Web App)
- 7) Install and configure **Snort IDS**.
- 8) Conduct basic **Metasploit penetration testing** on a test system.
- 9) Use **Autopsy and FTK Imager** to analyze a forensic image.
- 10) Implement **best practices for OS hardening (Windows/Linux)**.

List of open Source software/learning Websites:

- **Kali Linux** – <https://www.kali.org>
- **Wireshark** – <https://www.wireshark.org>
- **Metasploit Framework** – <https://www.metasploit.com>
- **TryHackMe** – <https://www.tryhackme.com>
- **Cybrary** – <https://www.cybrary.it>

* * * * *