Gyanmanjari
Innovative University

Course Syllabus
Gyanmanjari Institute of Technology
Semester-5 (Diploma)

Subject: Information & Network Security - DETCE15214

Type of Course: Professional Core

Prerequisite: Mathematical concepts: Random numbers, Number theory, finite fields

Rationale: In the present computing era, where the internet is the backbone of connectivity, information security is crucial for safeguarding sensitive data and protecting individuals, organizations, and nations from diverse cyber threats. This course emphasizes the importance of protecting confidentiality, preserving data integrity, ensuring availability, mitigating risks, and protecting privacy in the digital world.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
CI	T	P	C	Theory Marks		Practical Marks		CA	
				ESE	MSE	V	P	ALA	
4	0	2	5	60	30	10	20	30	150

Legends: CI-Classroom Instructions; T – Tutorial; P - Practical; C – Credit; ESE - End Semester Examination; MSE- Mid Semester Examination; V – Viva; CA - Continuous Assessment; ALA- Active Learning Activities.

Course Content:

Sr. No	Course Content	Hrs.	% Weightage
1	Introduction to Information Security Information Security: Definition, Importance, CIA Triad : Confidentiality, Integrity, Availability, Types of Threats: Internal & External, Types of Attacks: Passive & Active, Security Services: Authentication, Access Control, Data Integrity, Non-repudiation, Components of an Information Security System	12	20%
2	Cryptography Fundamentals Basics of Cryptography: Encryption, Decryption, Keys, Symmetric Key Algorithms: Caesar Cipher, DES, AES, Asymmetric Key Algorithms: RSA, Hashing Techniques: MD5, SHA, Digital Signatures and Certificates, Public Key Infrastructure (PKI)	14	25%
3	Network Security Concepts Network Security Model and Need, IP Security (IPSec) and SSL/TLS, Virtual Private Network (VPN) – Basics, Firewalls – Types and Functionality, Proxy Servers and NAT, Wireless Security – WEP, WPA, WPA2	12	20%
4	Threats, Attacks & Prevention Techniques Malware Types: Virus, Worm, Trojan, Ransomware, Spyware, Social Engineering and Phishing, DoS and DDoS Attacks, Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS), Antivirus and Anti-spyware Tools, Security Updates and Patch Management	14	20%
5	Cyber Law & Ethical Security Practices Overview, Types of Cybercrimes, Ethical Hacking – Concepts and Roles, Importance of Cyber Ethics and Safe Practices, Case Studies on Real Cybercrime Incidents	10	15%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Password Security and Modern Authentication Techniques** In groups of 5, explore password security and compare traditional vs. modern authentication methods (e.g., MFA, biometrics, OTP). Research common attacks like brute force, dictionary attacks, and credential stuffing. Implement a basic password strength checker or hashing demo (e.g., in Python). Include real-world breach case studies	10

GYANMANJARI INNOVATIVE UNIVERSITY • BHAVNAGAR

	(e.g., LinkedIn, Yahoo) and suggest best practices. Submit a structured PDF report on the GMIU portal.	
2	**Network security threats and firewall implementations** In groups of 5, research network security threats and firewall implementations. Analyze threat types, their impact, and how firewalls mitigate them. Include real-world case studies, compare firewall technologies, and suggest best practices. Submit a PDF report to the GMIU web portal.	10
3	**Simulating Network Security Concepts** Use Wireshark or Cisco Packet Tracer to capture and analyze network traffic, identify vulnerabilities, and study protocol behaviors. Document findings with screenshots and explanations, and submit a group report (5 students) as a PDF on the GMIU portal.	10
	Total	30

Suggested Specification table with Marks (Theory):60

Distribution of Theory Marks **(Revised Bloom's Taxonomy)**						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage %	15%	20%	25%	20%	10%	10%

Course Outcome:

After learning the course the students should be able to:	
CO1	Understand the fundamentals of Information Security, its principles, and real-world applications
CO2	Implement cryptographic techniques for securing data transmission and storage.
CO3	Apply symmetric and asymmetric encryption techniques in practical scenarios.
CO4	Identify various network security threats and implement appropriate protection measures.
CO5	Recognize and mitigate cyber security risks using tools like firewalls and IDS.

GYANMANJARI INNOVATIVE ... BHAVNAGAR

List of Practical

Sr. No	Description	Unit No.	Hrs.
1	Execute basic TCP/IP utilities and commands (ping, ipconfig, nslookup, telnet, etc.)	1	2
2	Implement Caesar Cipher for basic encryption and decryption. (Any of the Language C/C++/Java/Python)	2	4
3	Write a Program to implement Hill Cipher for basic encryption techniques.(Any of the Language C/C++/Java/Python)	2	4
4	Write a Program to implement the Play-Fair Cipher Technique for encryption. (Any of the Language C/C++/Java/Python)	2	4
5	Implement the RSA algorithm for asymmetric encryption. (Any of the Language C/C++/Java/Python)	3	2
6	Analyze network traffic using Wireshark.	4	4
7	Simulate network security concepts like VLAN and DMZ using Cisco Packet Tracer	4	4
8	Implement a simple firewall using Cisco Packet Tracer.	4	4
9	Study various types of cyber threats and mitigation techniques.	5	2
		Total	30

Instructional Method:

The course delivery method will depend upon the requirement of content and the needs of students.The teacher, in addition to conventional teaching methods by black board, may also use any tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in the laboratory. performance of students in laboratory.

Reference Books:

[1] Network Security Bible – Eric Cole

[2] Information Security Principles and Practice By Mark Stamp, Willy India Edition

[3] Network Security Essentials – William Stallings

[4] Cybersecurity for Beginners – Raef Meeuwisse

[5]Cryptography And Network Security, Principles And Practice Sixth Edition, William

GYANMANJARI INNOVATIVE UNIVERSITY • BHAVNAGAR