GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Industry Led Minor/Hons.

Level: UG

Branch: Cyber Security

Course / Subject Code : BE05IAQ011

Course / Subject Name : Network Security & Identity Management

w. e. f. Academic Year:	2025-26
Semester:	5
Category of the Course:	Core Subject

Prerequisite:	• Basic knowledge of computer Networks • Introduction to Cyber Security • Access Management Basics
Rationale:	This course provides essential knowledge in networking, security protocols, and identity management. It builds foundational skills in protecting networks, managing access, and effective security communication—key areas in cybersecurity.

Course Outcome:

After Completion of the Course, Student will be able to:

No	Course Outcomes	RBT Level
01	Predict data flow and understand network topology requirements.	N
02	Configure network devices and verify network operations.	A
03	Learn basics of network security, including threat prevention and management.	U
04	Understand attacks such as DoS, gaining access, and exploitation.	U
05	Implement defense techniques with firewalls, IDS, and IPS	A
06	Differentiate information security objectives and terminology.	N
07	Comprehend symmetric and asymmetric cryptography, hashing, and digital signatures.	U

**Revised Bloom's Taxonomy (RBT)*

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Industry Led Minor/Hons.

Level: UG

Branch: Cyber Security

Course / Subject Code : BE05IAQ011

Course / Subject Name : Network Security & Identity Management

Teaching and Examination Scheme:

Teaching Scheme (in Hours/week)			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
3	0	2	4	100				100
*Total Lecture Hrs. (L) =45			Total Practical Hrs. (PR) =30.			Total Hours =75 Hrs		

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**Network Fundamentals** - Introduction to Network, Networking Models, Cables, Network Topologies	10	20
2.	IP Addressing, Protocols and Utilities, Introduction to Router, Router Basics	10	10
3.	**Network Security-** Introducing Network Security, Network Scanning and Information Gathering, Attacks on Networks, Networks Security Tools and Techniques **Fundamentals of Information Security** - Why Information security? What is Information security? Data Security, Network security, Application Security	15	20
4.	**Identity Governance and Administration -** Need for IGA & basics concepts, IGA Basic Concepts and Onboarding, IGA Governance, Identity Administration in IGA, What next? **Identity and Access Management IAM -** Introduction to Identity and Access Management, What next	15	20
5.	**Communicating to Succeed:** Articulation Skills, Body Language - Change how people see you, Active Listening Skills, Barriers to Effective Listening, Email Etiquette, Basics of Email Writing, Design thinking Basics of Threat Modeling, What is Threat Modeling? Need for Threat Modeling, When Would One Do Threat Modeling? Threat	25	30

	Modeling Approach, Learn Threat Modeling with a Use Case, Use Case, Threat Rating - DREAD, Countermeasures, Tool Walkthrough - MS Threat Modeling Tool, Why is a tool needed? Threat Modeling Tools, Components that Make Up a Threat Model, Incorrect vs Correct data flow diagram,2mRules for Drawing a Model, Drawing Threat Model in MS Threat Modeling Tool		
	Total	**75**	**100**

Suggested Specification Table with Marks : Given here tentative, which may vary as per Author and Course.

Distribution of Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20%	**30%**	**20%**	**10%**	**10%**	**10%**

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

Skill & Practical Activities to be carried out during Semester

Important Note:- Please keep only applicable categories relevant to your offerings in this table and delete not applicable categories"

Sr. No.	Category of Engagement	Describe the activities to be carried out by students in brief	Expected Frequency & Duration	Mode of Delivery (Online / Offline / Hybrid)	Tools / Platforms / Equipment / Machinery to be Used	Expected major Learning Outcomes in 2 or 3 bullet points
1	Tutorials / Guided Technical Sessions	Hands-on sessions on IP addressing, firewalls, IDS/IPS	Weekly (2 hrs)	Offline / Online	Wireshark, Firewall tools	• Configure network devices • Analyze traffic
2	Master Classes / Expert Lectures by Industry Professionals	Attend the live class, ask doubt and	5 Days Master class twice in a	Online	Webex/Zoom	• Understand latest security practices

		complete practical	semester (20 Hours)			• IAM best practices
3	Quizzes	Complete quizzes on portal	After each module	online	Infosys springboard platform/app	Better understanding about topic
4	Hands-on Training / Lab Exercises / Tool-Based Learning	Configure routers, firewalls, and implement encryption	Weekly (2 hrs)	Offline	Cisco Packet Tracer, OpenSSL	• Secure network setup • Implement cryptography

* * * * * * *