GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)
Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)
Semester-V
Course Title: Cyber Security
(Course Code:4353204)

Diploma Programme in which this course is offered	Semester in which offered
Information and Communication technology	Fifth

1. RATIONALE

In an era defined by pervasive digital connectivity, Cyber Security stands as a vital shield against the ever-evolving landscape of cyber threats. Mastery of Cyber Security principles and tools transcends specific programming languages yet demands their application for effective defense strategies. This discipline is integral to the education of Information & communication technology, synergizing with other programming courses to foster a holistic understanding of software development. By equipping students with the expertise to identify, mitigate, and combat cyber risks, Cyber Security education cultivates responsible professionals capable of safeguarding critical data and infrastructures in our interconnected world.

2. COMPETENCY

The course content should be taught to cultivate competencies aimed at fortifying Cyber Security capabilities, leading to the attainment of the following proficiency:

● Apply diverse Cyber Security frameworks and methodologies for threat detection and mitigation within real-world scenarios.

3. COURSE OUTCOMES (COs)

The practical exercises, the underpinning knowledge and the relevant soft skills associated with this competency are to be developed in the student to display the following COs:

The practical experiences and relevant soft skills associated with this course are to be taught and implemented, so that the student demonstrates the following industry-oriented COs associated with the above-mentioned competency:

a) Understand the fundamental principles of cybersecurity, apply them to analyze, evaluate, and implement effective security measures in digital environments.
b) Implement security strategy encompassing authentication, authorization, defense against malicious software.
c) Secure web communications and applications by applying security protocols, managing ports, and implementing HTTPS, SSH, and VPN technologies.
d) Conduct ethical hacking and protect systems using Kali Linux tools and vulnerability assessment techniques.
e) Identify types of cybercrimes, understand their impact, and apply forensic techniques to investigate and prevent cyber-criminal activities.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T+P/2)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	CA	ESE	CA	ESE	
3	0	2	4	30*	70	25	25	150

(*):Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

Legends: ***L****-Lecture;* ***T*** *– Tutorial/Teacher Guided Theory Practice;* ***P*** *-Practical;* ***C*** *– Credit,* ***CA*** *- Continuous Assessment;* ***ESE*** *-End Semester Examination.*

5. SUGGESTED PRACTICAL EXERCISES

Following practical outcomes (PrOs) are the sub-components of the Course Outcomes (Cos). Some of the **PrOs** marked **'*'** are compulsory, as they are crucial for that particular CO at the 'Precision Level' of Dave's Taxonomy related to 'Psychomotor Domain'.

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
1.	Implement the following Substitution & Transposition Techniques concepts: a) Caesar Cipher b) Column Transformation	I	02
2.	Implement Private key Cryptography algorithm in python.	I	02
3.	Implement Message digest 5 and Secure Hash Function using python.	I	02
4.	Simulate a brute-force attack to crack passwords of varying strengths (weak, moderate, and strong) and measure the time it takes to crack each password. (Python code or any other tool)	II	02
5.	Set up squid proxy and Windows firewall to observe their effectiveness in blocking unauthorized network traffic.	II	02
6.	Create a Simple Packet Filter Script using *pydivert* package in python.	II	02
7.	Create malicious script for generating multiple folders using python.	II	02
8.	Create malicious script for keylogger using python. (use pynput package)	II	02

9.	Use Nmap to scan a network and identify open ports on a web server, then configure a firewall to block all ports except essential ones (e.g., 80 and 443), and use Nmap again to verify the configuration.	III	02
10.	a) Installation and configuration of Wireshark. b) Perform Password sniffing using Wireshark. (Analyse GET/POST Request)	III	02
11.	a) Installation and configuration of Kali Linux in Virtual box/VMware. b) Perform basic commands in Kali Linux.	IV	02
12.	Perform Memory forensic using Memoryze tool. (https://fireeye.market/apps/211368)	V	02
13.	Perform web Artifact analysis and registry analysis using Autopsy. (https://www.sleuthkit.org/autopsy/)	V	02
14.	Create forensic images of entire local hard drives using FTK IMAGER tool. (https://go.exterro.com/l/43312/2023-05-03/fc4b78)	V	02
			28 Hrs.

Note

i. *More **Practical Exercises** can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.*

ii. *Care must be taken in assigning and assessing study report as it is a first year study report. Study report, data collection and analysis report must be assigned in a group. Teacher has to discuss about type of data (which and why) before group start their market survey.*

The following are some **sample** 'Process' and 'Product' related skills (more may be added/deleted depending on the course) that occur in the above listed **Practical Exercises** of this course required which are embedded in the COs and ultimately the competency.

S.No.	Sample Performance Indicators for the PrOs	Weightage in %
1	Analyze and identify a suitable approach for the problem-solving	20
2	Use of appropriate technology/software/tools	25
3	Relevance and quality of output	25
4	Interpret the result and conclusion	15

5	Prepare a report/presentation for given problem/Viva	15
Total		**100**

6. MAJOR EQUIPMENTS/ INSTRUMENTS REQUIRED

These major equipment's with broad specifications for the PrOs is a guide to procure them by the administrators to user in uniformity of practical's in all institutions across the state.

S. No.	Equipment Name with Broad Specifications	PrO. No.
1	Computer system with operating system: Windows 10 or higher Ver., macOS, and Linux, with 4GB or higher RAM, Python versions: 3.7.X or higher	All
2	Python IDEs and Code Editors, Open Source: Anaconda Navigator, Autopsy, Openstego, FTK Imager, Wireshark, Nmap, Vmware, Kali Linux	All

7. AFFECTIVE DOMAIN OUTCOMES

The following ***sample*** Affective Domain Outcomes (ADOs) are embedded in many of the above-mentioned COs and PrOs. More could be added to fulfill the development of this course competency.

a) Work as a leader/a team member.
b) Follow ethical practices.
c) Practice environment friendly methods and processes.
d) Follow safety precautions.

The ADOs are best developed through the laboratory/field based exercises. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

i. 'Valuing Level' in 1st year
ii. 'Organization Level' in 2nd year.
iii. 'Characterization Level' in 3rd year.

8. UNDERPINNING THEORY

The major underpinning theory is given below based on the higher level UOs of *Revised Bloom's taxonomy* that are formulated for development of the COs and competency. If required, more such UOs could be included by the course teacher to focus on attainment of COs and competency.

Unit	Unit Outcomes (UOs) (4 to 6 UOs at different levels)	Topics and Sub-topics

Unit – I Introduction to Cyber security & Cryptography	1a Define cyber security and its importance in protecting digital assets and information. 1b Explain the CIA triad (Confidentiality, Integrity, Availability) and its significance in designing secure systems. 1c Define key terms such as adversary, attack, countermeasure, risk, security policy, system resource, threat, and vulnerability in the context of computer security. 1d Identify common security attacks, mechanisms, and services associated with each layer of the OSI model. 1e Explain the principles behind asymmetric encryption and how it enhances data security in various scenarios. 1f Understand how hashing algorithms are used to ensure data integrity and authentication in digital communications and storage systems.	1.1 Overview of Cyber Security: Definition, importance, and evolution. 1.2 Basic concept of computer security: CIA tirad. 1.3 Computer Security Terminology: Adversary (threat agent), Attack, Countermeasure, Risk, Security Policy, System Resource (Asset), Threat, Vulnerability 1.4 The OSI Security Architecture (security attacks, mechanisms, and services) 1.5 Private & Public Key Cryptography 1.6 MD5 hashing & SHA
Unit– II Account & Data Security	2a Define authentication and its significance in cybersecurity. 2b Define authorization and its significance in cybersecurity. 2c Explain different types of malicious software and their effect. 2d Explain different types of attack on account and data.	2.1 Authentication definition and methods: Password, Biometrics, Multi-factor authentication, SSO & cookies 2.2 Authorization definition and methods: CAPTCHA, Firewalls (packet filter, application proxy, personal firewall) 2.3 Malicious software: virus, worm, trojan horse, logical bomb, keylogger, sniffer, backdoor 2.4 Types of attacks: Brut force attack, Credential stuffing, Social Engineering, Phishing, vishing, Machine in the middle attack

Unit– III **Network & System Security**	3a Explain the impact of web security threats on integrity, confidentiality and authentication. 3b Explain the importance of network ports and identify key ports such as 80 (HTTP) and 443 (HTTPS) in web security. 3c Explain SSL and TLS protocols to encrypt data transmissions, ensuring secure communication over networks. 3d Describe the role of digital signatures and digital certificates. 3e Explain how VPNs create secure, encrypted connections over public networks to ensure privacy and data protection for remote users.	3.1 Web Security threats: Integrity, Confidentiality, Denial of service, Authentication 3.2 Ports: importance of ports, types, example (443,80 etc) 3.3 Secure Socket Layer and Transport Layer Security 3.4 Digital signatures & Digital certificates 3.5 HTTPS 3.6 SSH (secure shell), WAP END-TO-END SECURITY 3.7 VPN (Virtual Private Networks)
Unit– IV Ethical Hacking	4a Understand the ethical behavior with unethical behavior. 4b Understand basic terminology as it relates to the Kali Linux distribution. 4c To learn about various types of attacks, attackers and security threats and vulnerabilities. 4d To learn about scanning of systems/applications and System Protection.	4.1 Concept of Hacking Types of Hackers 4.2 Basics of Ethical Hacking 4.3 The terminology of Hacking (Vulnerability, Exploit, 0-Day) 4.4 Five Steps of Hacking (Information Gathering, Scanning, Gaining Access, Maintaining Access, Covering Tracks) 4.5 Information Gathering (Active, Passive) 4.6 Introduction to Kali Linux OS , Configuration of Kali Linux ,Basic Commands Kali Linux, Vulnerability Scanning/ Vulnerability Based Hacking a. Foot printing b. Scanning c. Password Cracking d. Brute Force Attacks e. Injection Attacks f. Phishing Attacks g. Block chain Attacks 4.7 Port Scanning 4.8 Remote Administration Tool (RAT) 4.9 Protect System from RAT

		4.10 What is Sniffing and Mechanism of Sniffing Session Hijacking
Unit– V Cyber Crime & Cyber forensic	5a Understand the cybercrimes from the nature of the crime. 5b Analyze various aspects of Cyber-crimes. 5c Understand the security and privacy methods in development of modern applications and in organizations to protect people and to prevent cybercrimes. 5d Analyze how particular social engineering attacks are important consideration for cyber security 5e Describe the basic concepts of Forensic and Branches of Digital Forensic.	5.1 Introduction to Cyber Crime – Types of Cyber Crime 5.2 Classification of Cyber Crimes: 5.2.1. Organization: Email Bombing, Salami Attack, Web Jacking, Data diddling, Distributed Denial of Service, Ransomware 5.2.2. Individual: Cyber bullying, Cyber stalking, Cyber defamation, Cyber fraud and Cyber theft, Spyware, Email spoofing, Man in the middle attack 5.2.3. Society: Cyber terrorism, cyber spying, Social Engineering Attack, Online gambling 5.2.4. Property: Credit Card Fraud, Software Piracy, Copyright, infringement, Trademarks violations 5.3 Challenges & Prevention of Cyber Crime 5.4 Cyber Forensics Definition, 5.5 Overview: Disk Forensics, Network Forensics, Wireless Forensics, Database Forensics, Malware Forensics, Mobile Forensics, Email Forensics

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Introduction to Cyber security & Cryptography	8	4	4	4	12
II	Account & Data Security	7	2	6	4	12

III	Network & System Security	8	4	8	3	15
IV	Ethical Hacking	9	2	7	4	13
V	Cyber Crime & Cyber forensic	10	4	10	4	18
Total		**42**	**16**	**35**	**19**	**70**

Legends: *R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)*

10. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related ***co-curricular*** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare small reports (of 1 to 5 pages for each activity). For micro project report should be as per suggested format, for other activities students and teachers together can decide the format of the report. Students should also collect/record physical evidences such as photographs/videos of the activities for their (student's) portfolio which will be useful for their placement interviews:

a) Provide students with real-world case studies of cyber attacks and have them analyze the incidents, identify vulnerabilities exploited, and suggest mitigation strategies..

b) Organize competitions where students can practice ethical hacking skills and solve security challenges.

c) Develop and conduct an awareness campaign on cybersecurity best practices for the campus community, including creating informative posters, videos, and presentations.

d) Students are encouraged to register themselves in various MOOCs such as: Swayam, edx, Coursera, Udemy etc. to further enhance their learning.

e) Undertake micro-projects to develop simple security tools, such as password generators, encryption/decryption programs, or network monitoring tools.

f) Organize guest lectures and workshops with industry professionals to provide insights into the latest trends, challenges, and technologies in cybersecurity.

g) Conduct security audits of the institute's IT infrastructure under supervision, identifying potential vulnerabilities and suggesting improvements.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

a) Massive open online courses (***MOOCs***) may be used to teach various topics/sub topics.
b) Guide student(s) in undertaking micro-projects.
c) Managing Learning Environment
d) Diagnosing Essential Missed Learning concepts that will help for students.
e) Guide Students to do Personalized learning so that students can understand the course material at his or her pace.
f) Encourage students to do Group learning by sharing so that teaching can easily be enhanced.
g) ***'L" in section No. 4*** means different types of teaching methods that are to be employed by teachers to develop the outcomes.
h) About ***20% of the topics/sub-topics*** which are relatively simpler or descriptive in nature is to be given to the students for ***self-learning***, but to be assessed using different assessment methods.
i) With respect to ***section No.10***, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.
j) Guide students on how to address issues on environment and sustainability using the knowledge of this course

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-project are group-based (group of 3 to 5). However, **in the fifth and sixth semesters**, the number of students in the group should ***not exceed three.***

The micro-project could be industry application based, internet-based, workshop- based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain dated work diary consisting of individual contribution in the project work and give a seminar presentation of it before submission. The total work load on each student due to the micro-project should be about ***16 (sixteen) student engagement hours*** (i.e., about one hour per week) during the course. The students ought to submit micro-project by the end of the semester (so that they develop the industry-oriented COs).

A suggestive list of micro-projects is given here. This should relate highly with competency of the course and the COs. Similar micro-projects could be added by the concerned course teacher:

a) Create a script that configures basic firewall rules using iptables to block or allow specific types of network traffic.
b) Develop a Python-based web application that incorporates password-based authentication and an additional factor like OTP (One-Time Password) or biometric authentication.
c) Write a Python program using libraries like Scapy to capture and analyze network packets for monitoring network traffic.
d) Develop a simulation that demonstrates a basic DoS attack on a server and implement measures to detect and mitigate such attacks.
e) Develop a Python program that monitors system logs and network traffic for suspicious activities and generates alerts.
f) Create a tool that scans web applications for common vulnerabilities such as SQL injection, XSS (Cross-Site Scripting), and weak authentication mechanisms.

g) Implement a Python program that uses the paramiko library to securely transfer files between a client and server using the SSH protocol.
h) Write a script to set up and configure a secure VPN server using OpenVPN, and demonstrate secure remote access to a network.
i) Create a Python program that generates digital signatures for documents and verifies their authenticity using public key infrastructure (PKI).

13. SUGGESTED LEARNING RESOURCES

S. No.	Title of Book	Author	Publication with place, year and ISBN
1	Information security Principles and practice	Mark Stamp	Wiley, 2006 ISBN-10 0-471-73848-4
2	Cryptography & Network Security: Principles & Practice	William Stallings	Pearson, 2019, ISBN 10: 0-13-576403-3
3	Computer security: Principles and Practice	William Stallings	Pearson ,2017, ISBN-10: 0-13-479410-9
4	Introduction to Cyber Security	Dr. Jeetendra Pande	Uttarakhand Open University , 2017, ISBN-978-93-84813-96-3
5	Handbook Of Digital Forensics and Investigation	Eoghan Casey	Elsevier, 2010, ISBN-978-0-12-374267-4
6	Ethical Hacking	Daniel Graham	No Starch Press, 2021, ISBN-13: 978-1-7185-0187-4
7	Penetration Testing: A hands on introduction to hacking	Georgia Weidman	No Starch Press, 2014, ISBN-10: 1-59327-564-1

14. SOFTWARE/LEARNING WEBSITES

1. https://www.edx.org/learn/cybersecurity/harvard-university-cs50-s-introduction-to-cybersecurity
2. https://www.geeksforgeeks.org/types-of-cyber-attacks/
3. https://onlinecourses.nptel.ac.in/noc22_cs13/preview
4. https://www.tutorialspoint.com/ethical_hacking/index.htm
5. https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/
6. https://csrc.nist.gov/
7. https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
8. https://www.dsci.in/content/dsci-security-framework-dsf

9. https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html

15. PO-COMPETENCY-CO MAPPING

Semester III	Cyber Security						
	Pos						
Competency & Course Outcomes	**PO 1 Basic & Discipline specific knowledge**	**PO 2 Problem Analysis**	**PO 3 Design/ development of solutions**	**PO 4 Engineering Tools, Experimentation & Testing**	**PO 5 Engineering practices for society, sustainability & environment**	**PO 6 Project Management**	**PO 7 Life-long learning**
Competency	**Apply diverse Cyber Security frameworks and methodologies for threat detection and mitigation within real-world scenarios**						
Course Outcomes CO a)Understand the fundamental principles of cybersecurity, apply them to analyze, evaluate, and implement effective security measures in digital environments.	3	3	2	1	-	-	1
CO b) Implement security strategy encompassing authentication, authorization, defense against malicious software.	-	2	1	2	1	1	-
CO c) Secure web communications and applications by applying security protocols, managing ports, and implementing	1	-	3	1	2	-	2

HTTPS, SSH, and VPN technologies.							
CO d) Conduct ethical hacking and protect systems using Kali Linux tools and vulnerability assessment techniques.	2	2	-	3	-	2	3
CO e) Identify types of cyber crimes, understand their impact, and apply forensic techniques to investigate and prevent cyber criminal activities.	2	2	1	1	2	-	3

*Legend: '**3**' for high, '**2**' for medium, '**1**' for low and '**-**' for no correlation of each CO with PO.*

16. COURSE CURRICULUM DEVELOPMENT COMMITTEE

GTU Resource Persons

Sr. No.	Name and Designation	Institute	Contact No.	Email
1.	Ashish M Patel, Lecturer in EC	Government Polytechnic For Girls, Surat	9924050239	gpgsecamp@gmail.com