GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)
Semester -VI

Course Title: Cyber Security and Digital Forensics
(Course Code:4361601)

Diploma Programme In Which This Course Is Offered	Semester In Which Offered
Information Technology	6th semester

1. RATIONALE

Cyber security and digital forensics are two essential disciplines in the field of information technology. Cyber Security and Digital Forensics is essential to address the critical shortage of professionals in these fields. This curriculum equips students with the knowledge and skills needed to protect sensitive data, understand the legal and ethical aspects of digital investigations, and pursue diverse career opportunities in information security and digital forensics. Furthermore, it contributes to national security by preparing professionals to defend critical digital infrastructure and fosters adaptability to emerging threats and technologies in the ever-evolving digital landscape.

This curriculum ensures that graduates are not only technically proficient but also ethically responsible professionals who can play a crucial role in protecting digital assets, solving digital crimes, and contributing to the broader field of information technology and security.

2. COMPETENCY

The purpose of this course is to help the student to attain the following industry identified competency through various teaching-learning experiences:

- Enhance knowledge of the latest cyber security threats, attacks, crimes and technologies for prevent them.
- Demonstrate advanced practical skills in hacking tools and cybercrime investigation.

3. Course Outcomes:

After completing the course, the students will be able to

a) Gain knowledge of information security, including Cryptography and hashing techniques.
b) Explain the different types of network and system security techniques and threats.
c) Understand the different types cybercrimes and Analyse cybercrime.
d) Implement ethical hacking methodologies using Kali Linux, including vulnerability analysis.
e) Explain how digital forensics methodologies use for investigate cybercrimes.

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	
4	-	4	6	30	70	25	25	150

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

Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project To facilitate the 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.

5. SUGGESTED PRACTICAL EXERCISES

The following practical outcomes (PrOs) that are the subcomponents of the Cos.

Sr. No.	Practical Outcomes (PrOs)	Approx. Hrs. required	Unit No.
1	a) Implement Private key Cryptography algorithm DES in python. (Install des package using pip) b) Implement Message digest 5 and Secure Hash Function using python.	4	1
2	Implement the RSA Public key Cryptography algorithm in Python using RSA library.	4	1
3	Demonstrate intrusion detection system (ids) using any tool.(snort or any other s/w)	4	2
4	Install Tor browser and perform proxy tunnelling.	4	2
5	Perform data hiding using Steganography tool Openstego (use AES encryption algorithm).	4	3
6	Create malicious script for generating multiple folders using python.	4	3
7	Prepare a case study report on 3 different types of cyber-crimes. (https://gujaratcybercrime.org) (https://cybercrime.gov.in)	4	3
8	Study Open-source intelligence (OSINT) framework and perform Information gathering using Username, Email address , Domain name and IP address.	4	4
9	a) Installation and configuration of Kali Linux in Virtual box/VMware. b) Perform basic commands in Kali Linux.	4	4
10	Perform port scanning using NMAP.	4	4
11	a) Installation and configuration of Wireshark. b) Perform Password sniffing using Wireshark. (Analyse GET/POST Request)	4	5
12	Perform Memory forensic using Memoryze tool. (https://fireeye.market/apps/211368)	4	5
13	Perform web Artifact analysis and registry analysis using Autopsy. (https://www.sleuthkit.org/autopsy/)	4	5
14	Create forensic images of entire local hard drives using FTK IMAGER tool. (https://go.exterro.com/l/43312/2023-05-03/fc4b78)	4	5
	TOTAL Hrs.	**56**	

Note

*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.*

*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.*

Sr.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 EQUIPMENT/ INSTRUMENTS AND SOFTWARE REQUIRE

Sr. No.	Equipment Name with Broad Specifications	PrO. No.
1	Computer system with operating system: Windows 7 or higher Ver.,macOS,and KaliLinux,with4GBorhigherRAM,Pythonversions: 2.7.X, 3.6.X	All
2	Python IDEs and Code Editors, Goolge Colab Platform, Open Source: Anaconda Navigator, Autopsy, Openstego, FTK Imager, Wireshark, Nmap	

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 fulfil the development of this competency.

a) Work as a leader/team member.
b) Follow ethical practices for cyber security

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

Unit No.	UNIT OUTCOMES	Topics and Sub-topics
Unit – I Introduction of Information Security and Cryptography	1a. Learn about how to maintain the Confidentiality, Integrity and Availability of a data. 1b. Analyze and design hash and MD5 algorithms.	1.1. Basic Concept of Information Security 1.2. CIA Triad 1.3. OSI Security Architecture (Security Services, Mechanisms and Attacks) 1.4. Private & Public Key Cryptography 1.5. Message Digest 5 Hashing & SHA
Unit– II Network and System security	2a. To understand various protocols for network security to protect against the threats in the networks. 2b. Understand the threats and risks to modern data and information systems. 2c. Understand the working and configuration of firewall.	2.1. Types of attacks 2.2. Digital signatures: Definition and Properties 2.3. Pretty Good Privacy (PGP)(brief) 2.4. Secure Socket Layer and Transport Layer Security 2.5. IPsec 2.6. HTTPS (Connection initiation & Connection closure) 2.7. Malicious software: Virus and Related Threats (Trojans, Rootkit, Backdoors, keylogger) 2.8. Firewall :Need and Types 2.9. Proxy Server: Need and Types
Unit– III Cyber Crime	3a. Understand the cybercrimes from the nature of the crime.	3.1 Overview of Cybercrime • Definition • Cybercriminals

	3b. Analyze various aspects of Cyber-crimes. 3c. Understand the security and privacy methods in development of modern applications and in organizations to protect people and to prevent cyber-crimes. 3d. Analyze how particular social engineering attacks are important consideration for cyber security. 3e. Understand the Objectives and features of IT ACT, 2008.	• Cybercrime 3.2 Classification of cyber-crimes 3.2.1. Organization a. Email Bombing b. Salami Attack c. Logic Bomb d. Trojan Horse e. Web Jacking f. Data diddling g. Denial of Service/ Distributed Denial of Service h. Ransomware 3.2.2. Individual a. Cyber bullying b. Cyber stalking c. Cyber defamation d. Phishing e. Cyber fraud and Cyber theft f. Spyware g. Email spoofing h. Man in the middle attack 3.2.3. Society a. Cyber pornography b. Cyber terrorism c. cyber spying d. Social Engineering Attack e. Online gambling 3.2.4. Property a. Credit Card Fraud b. Software Piracy c. Copyright infringement d. Trademarks violations 3.3 Challenges & Prevention of Cyber Crime 3.4 Cyber Law The Information Technology ACT, 2008 OFFENCES • Section 65 • Section 66 • Section 67
Unit– IV Ethical Hacking	4a. Understand the ethical behaviour with unethical behaviour. 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.	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

	4d. To learn about scanning of systems/applications and System Protection.	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 DIGITAL FORENSICS	5a. Describe the basic concepts of Forensic and Branches of Digital Forensic. 5b. Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective. 5c. To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices. 5d. To understand how to examine digital evidences such as the data acquisition, identification analysis.	5.1. Introduction to Digital Forensics 5.2. Locard's Principle of Exchange in Digital Forensics 5.3. Branches of Digital Forensics • Disk / Memory Forensics • Network Forensics • Database Forensics • Software forensics • Email Forensics • Malware Forensics • Mobile Forensics 5.4. Phases of digital/computer forensics investigation • Identification • Preservation • Analysis • Documentation • Presentation 5.5. Methods to Preserve a Digital Evidence • Drive Imaging • Hash Values • Chain of Custody 5.6. Critical Steps in Preserving Digital Evidence 5.7. Evidence Role of devices as in Digital Forensics Investigations • Computing Devices • Network Devices and Servers • CCTV • Vehicles

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	Overview of Information Security and Cryptography	8	4	4	4	12
II	Network and System Security	10	2	4	6	12
III	Cyber Crime	12	2	6	6	14
IV	Ethical Hacking	14	4	6	6	16
V	Digital Forensics	12	2	8	6	16
	Total	**56**	**12**	**30**	**28**	**70**

Legends: *R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)*
Note*: This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from the above table.*

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 reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

a) Start or join a cyber security club or team on your campus.

b) Undertake hacking and cybercrime investigation assignments/micro-projects in teams.

c) Organize or attend workshops and training sessions on topics like ethical hacking, penetration testing, cybercrime and digital forensics.

d) Invite industry professionals and experts to give talks and presentations on the latest trends and best practices in cyber security and digital forensics.

e) Visit your nearest Gujarat government cybercrime department and learn how investigate cybercrime.

f) Organize campaigns to promote cyber security awareness and best practices on your campus.

g) Identify the vulnerable points for attacks in simple networks in your college and college websites/government websites.

h) Collect and analyze information regarding various types of cyber-attacks and cyber fraud and provide solution to prevent it

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

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES

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/subtopics.

b) Guide student(s) in undertaking micro-projects.

c) ***'L' in section No. 4*** means different types of teaching methods that are to be employed by teachers to develop the outcomes.

d) 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.

e) With respect to ***section No.11***, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a students that needs to be assigned to them in the beginning of the semester. The number of students in the group should not exceed three. The micro-project could be industry application based, internet-based, workshop based, incident 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 a dated work diary consisting of individual contributions in the project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than 16 (sixteen) student engagement hours during the course. The student ought to submit a micro-project by the end of the semester to develop the industry-oriented COs.

A suggestive list of micro-projects is given here. This has to match the competency and the COs. Similar micro-projects could be added by the concerned course teacher:

Idea 1:Anomaly Detection System: Build an anomaly-based DDoS detection system that establishes a baseline of normal network behaviour and identifies deviations from this baseline as potential attacks. This could involve statistical analysis or machine learning techniques.

Idea 2:Credit Card Fraud Detection System: Develop an intelligent credit card fraud detection system that combines various techniques and technologies to identify and prevent fraudulent credit card transactions in real-time. The system should be able to distinguish between legitimate transactions and unauthorized or fraudulent activities.

Idea 3:Create a Case Study: Ask students to analyze a genuine or hypothetical legal case that involves digital evidence and require them to create a comprehensive report or presentation focusing on the various aspects of digital forensics within the case.

Idea 4: **Network traffic logs analysis**:Provide network traffic logs for analysis by students to detect any potentially suspicious or malicious activities, including unauthorized access or data exfiltration.

Idea 5:**Basic mobile forensic analysis**: Students should be guided to perform a mobile forensic analysis, which involves extracting deleted text messages, phone records, and other digital evidence.

Idea 6: **Network Scanning & Vulnerability Assessment:** Prepare report and suggest ways to secure local area network or WLAN of institute.

Idea 7: Identify web application is vulnerable to something like SQL injection or XSS and suggest ways to protect it.

Idea 8: Use ethical hacking to break passwords.

13. SUGGESTED LEARNING RESOURCES

Sr. No	Title of Book	Author	Publication with place, year and ISBN
1	Cryptography And Network Security	William Stallings	Pearson
2	Cyber security: The Hacker Proof Guide to Cyber security, Internet Safety, Cybercrime &Preventing Attacks	Leon Tietz	Trust Genics
3	Cyber Security Essentials	James Graham	CRC Press
4	Kali Linux Made Easy for Beginners And Intermediates	Berg Craig	Antony Mwau
5	Ethical Hacking	Daniel Graham	No Starch Press.
6	Handbook Of Digital Forensics and Investigation	Eoghan Casey	Academic Press

14. SUGGESTED LEARNING WEBSITES

a) https://www.malwarebytes.com/malware
b) https://www.javatpoint.com/firewall
c) https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/
d) https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/
e) https://www.geeksforgeeks.org/types-of-cyber-attacks/

f) https://www.javatpoint.com/cyber-security-tutorial
g) https://www.tutorialspoint.com/ethical_hacking/index.htm
h) https://www.startertutorials.com/blog/cyberforensics-and-digital-evidence.html
i) https://onlinecourses.nptel.ac.in/noc22_cs13/preview

15. PO-COMPETENCY-CO MAPPING

Semester VI	Cyber Security and Digital Forensic(CourseCode:4361603)						
	Pos and PSOs						
Competency & Course Outcomes	PO 1 Basic & Discipline specific knowledge	PO 2 Problem Analysis	PO 3Design/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 • Enhance knowledge of the latest cyber security threats, attacks, crimes and technologies for prevent them. • Demonstrate advanced practical skills in hacking tools and cybercrime investigation.							
Course Outcomes **CO a)** Gain knowledge of information security, including Cryptography and hashing techniques.	1	-	-	1	-	-	1
CO b) Explain the different types of network and system security techniques and threats	-	2	1	1	-	-	2
CO c) Understand the different types cybercrimes and Analyse cybercrime.	-	3	1	2	1	1	3
CO d) Implement ethical hacking tasks using Kali Linux, including vulnerability scanning, penetration testing.	1	3	1	2	2	1	3
Co e) Explain how digital forensics methodologies use for investigate cybercrimes	-	2	1	3	2	1	2

Legend: '**3'**for high,'**2**' for medium,**'1'**for low or **'-'**for the relevant correlation of each competency, CO, with PO/ PSO

16. COURSE CURRICULUM DEVELOPMENT COMMITTEE

GTU Resource Persons

Sr. No.	Name and Designation	Institute	Email
1	Vikas H. Sitapara	L.E College (Diploma), Morbi	vikas9mobile@gmail.com
2	Jaydeep R. Tadhani	Government Polytechnic, Rajkot	jay.it2011@gmail.com
3	Snehalkumar I. Pate	Government Polytechnic for Girls, Ahmedabad	er.patelsnehal@gmail.com