GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Master of Computer Applications

Level: Post Graduate

Course / Subject Code: MC03094161

Course / Subject Name: Cyber Security and Forensic

w. e. f. Academic Year:	2024-25
Semester:	3
Category of the Course:	Elective Group - 2

Prerequisite:	• Basic knowledge of networking and operating systems • Understanding of computer architecture • Familiarity with programming and scripting (Python preferred)
Rationale:	Cyber security and forensic knowledge is indispensable in the era of increasing cyber threats. This course introduces foundational concepts of cyber security and digital forensics, empowering students to protect, detect, analyze, and respond to cyber incidents using open-source tools. It blends theoretical understanding with practical hands-on lab sessions, enhancing employability in security analysis and forensic investigation roles. **Course Pedagogy:** The course adopts an open-source-centric, hands-on pedagogy. It integrates real-world cyber-attack simulations, digital forensic case studies, and interactive lab sessions. Students will gain proficiency in threat detection, network security, and forensic analysis using tools like Wireshark, Autopsy, Volatility, and Kali Linux. Collaborative and problem-based learning strategies will be employed to simulate real cyber-incident handling.

Course Outcome:

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

No	Course Outcomes	RBT Level
01	Explain key concepts of cyber security, vulnerabilities, and threat landscape.	UN
02	Apply open-source tools to perform network traffic analysis and packet capture.	AP
03	Analyze and respond to cyber-attacks using forensic investigation techniques.	AN
04	Use digital forensic tools to recover and examine digital evidence.	AP
05	Evaluate the effectiveness of cyber defense mechanisms and report findings.	EL

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
2	0	2	3	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	Introduction to Cyber Security: Threats, Attacks, Vulnerabilities, CIA triad, Cyber Laws, Kali Linux Overview	9	20
2.	Network Security: Packet analysis using Wireshark, Firewalls, Snort for intrusion detection, DNS spoofing, ARP attacks	9	20
3.	System Security: Linux/Windows security, Malware analysis, Password cracking (John the Ripper, Hashcat), Metasploit	9	20
4.	Digital Forensics: Basics, Chain of custody, Disk imaging (dd, FTK Imager), Hashing, Timeline Analysis	9	20
5.	Forensic Tools and Reporting: Autopsy, Volatility, Registry analysis, Email and browser forensics, Report writing	9	20
	Total	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
10	20	25	15	15	15

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

References/Suggested Learning Resources:
(a) Reference Books:

1. William Stallings, "Network Security Essentials", Pearson
2. Nelson, Phillips, Steuart, "Guide to Computer Forensics and Investigations", Cengage
3. Chuck Easttom, "Computer Security Fundamentals", Pearson
4. Marjie T. Britz, "Computer Forensics and Cyber Crime", Pearson

(b) Online Learning Resources and Opensource software and website:

- NPTEL: Cyber Security and Forensics – https://nptel.ac.in/courses/106105197/
- Wireshark: https://www.wireshark.org/
- Kali Linux: https://www.kali.org/
- Autopsy: https://www.autopsy.com/
- Volatility Framework: https://www.volatilityfoundation.org/

- Snort IDS: https://www.snort.org/
- FTK Imager (Free Version): https://accessdata.com/product-download
- Hashcat: https://hashcat.net/
- John the Ripper: https://www.openwall.com/john/

Suggested List of Practical

1. Install and configure Kali Linux virtual environment
2. Perform network packet analysis using Wireshark
3. Scan and detect vulnerabilities using Nmap and OpenVAS
4. Simulate brute-force attack using Hydra and observe logs
5. Analyze a pcap file and report suspicious traffic
6. Crack password hashes using John the Ripper and Hashcat
7. Perform disk imaging and hashing using dd and sha256sum
8. Recover deleted files using Autopsy
9. Analyze memory dump using Volatility
10. Create a digital forensic investigation report

List of Active Learning Assignments:

1. Analyze and document a recent cyber-attack case
2. Perform a comparative analysis of different forensic tools (Autopsy vs Sleuthkit)
3. Simulate a network breach and write a detailed investigation report
4. Create a short video demo of recovering deleted files from a USB drive
5. Present a group-based discussion on the ethical and legal implications of cyber forensics

CO- PO Mapping:

Semester 3	**Course Name : Containerization**							
	POs							
Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	1	-	-	-	-	-
CO2	2	3	2	2	-	-	-	-
CO3	2	3	3	3	-	-	-	-
CO4	2	2	3	3	-	-	-	-
CO5	2	2	2	3	-	-	-	-

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

Note: The CO-PO mapping is indicative; the institute/faculty member can change as required.

* * * * * * *