COURSE CONTENT

CYBER SECURITY LAB								
II Semester: CSE								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
2525882	Foundation	0	0	4	2	40	60	100
Contact Classes: Nil	Tutorial Classes: Nil	Practical Classes: 60				Total Classes: 60		
Prerequisites: A course on "Network Security and Cryptography".								

Course Overview:

The Cyber Security Lab is a practical-oriented course designed to provide hands-on experience in identifying, analyzing, and mitigating security threats in computer systems and networks. The lab complements theoretical cybersecurity concepts by allowing students to work with real-world tools, attack simulations, and defensive mechanisms in a controlled environment.

Course Objectives:

1. To understand the fundamentals of cyber security threats, vulnerabilities, and attack techniques.
2. To develop practical skills in network scanning, traffic analysis, and intrusion detection using security tools.
3. To apply cryptographic techniques such as encryption, hashing, and digital signatures for secure communication.
4. To perform cyber forensic investigations using forensic analysis and monitoring tools.
5. To design and evaluate security mechanisms for protecting computer systems and networks from cyber-attacks.

Course Outcomes: After Completion of the Course, Students should be able to

1. Interpret scan results for responsible security assessment for the open services and associated vulnerabilities of the Network.
2. Design honeypot on a network to capture attacker activity and intrusion patterns for threat intelligence.
3. Demonstrate symmetric/asymmetric encryption, hashing, and digital/PKI signatures and verify message integrity/authenticity.
4. Build secure passwords programmatically using OpenSSL commands and evaluate password strength against common attack models.
5. Formulate network traffic using Wireshark to identify protocols, detect anomalies, and reconstruct sessions for forensic investigation.

List of Experiments.

1. Perform an Experiment for port scanning with NMAP.
2. Setup a honeypot and monitor the honeypot on the network.
3. Install Jcrpt /Cryptool tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures.
4. Generate minimum 10 passwords of length 12 characters using open SSL command.
5. Perform practical approach to implement Foot Printing-Gathering target information using Dmitry-Dmagic, UAtester.

6. Working with sniffers for monitoring network communication (Wireshark).
7. Use Snort to perform real time traffic analysis and packet logging.
8. Perform email analysis using Autopsy tool.
9. Perform Registry analysis and get boot time logging using process monitor tool
10. Perform File type detection using Autopsy tool.
11. Perform Memory capture and analysis using FTK imager tool.
12. Perform Network analysis using the Network Miner tool.

TEXT BOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010.

REFERENCE BOOKS:

1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A. Reyes, Syngress, 2007.

ELECTRONIC RESOURCES:

1. https://tryhackme.com/
2. https://www.cybrary.it/free-content/
3. https://labex.io/courses/cybersecurity-labs-for-beginners/
4. https://hacktivity.co.uk/hacktivities/121/

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)