SVKM's Mithibai College of Arts, Chauhan Institute of Science & Amrutben Jivanlal College of Commerce & Economics (AUTONOMOUS)

Program: B. Sc. - Computer Science				**Semester: VI**	
Course: Ethical Hacking & Cyber forensics				**Course Code:-new code**	
Teaching Scheme				**Evaluation Scheme**	
Lecture (Hours per week)	**Practical (Hours per week)**	**Tutorial (Hours per week)**	**Credit**	**Continuous Assessment and Evaluation (CAE) (Marks - 25)**	**Term End Examinations (TEE) (Marks-75 in Question Paper)**
04	03	-	4	25	75

Learning Objectives:

- To advance conceptual cognizance of ethics, legality, methodologies and techniques of hacking and the procedures for identification, preservation, extraction of electronic evidence, auditing and investigation of network and host system intrusions, analysis and documentation of information gathered.

Course Outcomes:

After completion of the course, learners will be able to:

CO1: Identify security vulnerabilities and weaknesses in the target applications.

CO2: Recognize to test and exploit systems using various tools and understand the impact of hacking in real time machines.

CO3: Plan and prepare for all stages of an investigation - detection, initial response and management interaction

CO4: Investigate various media to collect evidence, report them in a way that would be acceptable in the court of law.

Outline of Syllabus: (per session plan)

Module	**Description**	**No of hours**
1	Information Security: Attacks, Vulnerabilities and their prevention mechanisms	**15**
2	Ethical Hacking	**15**
3	Computer, Network, Cell Phone & Internet Forensic Forensics	**15**
4	E-mail Forensics, social media forensics & Investigations	**15**
	Total	**60**
PRACTICALS		**30**

Module	Topic	No. of Hours/Credits 60/4
1	**Information Security: Attacks, Vulnerabilities and their prevention mechanisms**	**15**
	Information Security: Attacks and Vulnerabilities Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Malware, Worms, viruses, Trojans, Spyware, Rootkits, Types of vulnerabilities: Top 10 OWASP. **Types of attacks and their common prevention mechanisms**: Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs Case-studies: Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit, Media Markt, Kaseya, JBS, Colonial Pipeline, The University of California at San Francisco.	
2	**Ethical Hacking**	
	Introduction: Ethical Hacking Terminology, Types of Hacking Technologies, Phases Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking, why is Ethical hacking needed? How is Ethical hacking different from security auditing and digital forensics? Vulnerability assessment and Penetration Testing, Application Security Testing, Phases, Foot printing and Social Engineering, Sniffers, systems hacking – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IP Spoofing, SYN Flooding, Smurf attack. Recent Case studies.	**15**
3	**Computer, Network, Cell Phone & Internet Forensic Forensics**	**15**
	Computer Forensics: Introduction to Digital Forensics and its phases, Preparing for Digital Investigations, Data Acquisition and Processing Crime Incident Scenes, Understanding File Systems and recovery, Data Encryption and Compression, Automated Search Techniques, Forensics Software **Network Forensic**: Introduction to Network Forensics and tracking	

	network traffic, Reviewing Network Logs, Network Forensics Tools, Performing Live Acquisitions, Order of Volatility, and Standard Procedure. **Cell Phone and Mobile Device Forensics**: Overview, Acquisition Procedures for Cell Phones and Mobile Devices **Internet Forensic**: Introduction to Internet Forensics, World Wide Web Threats, Obscene and Incident transmission, Domain Name Ownership Investigation, Reconstructing past internet activities and events	
4	**E-mail Forensics, social media forensics & Investigations**	**15**
	E-mail Forensics: e-mail analysis, e-mail headers and spoofing, Laws against e-mail Crime, Messenger Forensics: Yahoo Messenger **Social Media Forensics**: Social Media Investigations **Browser Forensics**: Cookie Storage and Analysis, Analyzing Cache and temporary internet files, Web browsing activity reconstruction **Investigation, Evidence presentation and Legal aspects of Digital Forensics**: Authorization to collect the evidence, Acquisition of Evidence, Authentication of the evidence, Analysis of the evidence, Reporting on the findings, Testimony, Report Writing for High-Tech Investigations **Introduction to Legal aspects of Digital Forensics:** Laws & regulations, Information Technology Act, Giving Evidence in court, Case Study – Cyber Crime cases, Case Study – Cyber Crime cases.	

PRACTICALS	
Sr. No.	**Topic.**
1	Port Scanning using NMap, Superscan
2	Use Wireshark (Sniffer) to capture network traffic and analyze.
3	Simulate persistent cross-site scripting attack.
4	Session impersonation using Firefox and Tamper Data add-on.

5	Perform SQL injection attack
6	simple keylogger using python
7	Creating a Forensic Image using FTK Imager/Encase Imager : - Creating Forensic Image - Check Integrity of Data - Analyze Forensic Image
8	Using Sysinternals tools for Network Tracking and Process Monitoring : - Check Sysinternals tools - Monitor Live Processes - Capture RAM - Capture TCP/UDP packets - Monitor Hard Disk - Monitor Virtual Memory - Monitor Cache Memory
9	Recovering and Inspecting deleted files - Check for Deleted Files - Recover the Deleted Files - Analyzing and Inspecting the recovered files Perform this using recovery option in ENCASE and also Perform manually through command line.
10	Email forensics using AccessData FTK

ESSENTIAL READING:

Textbook(s):

1) CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, Kimberly Graves
2) Guide to computer forensics and investigations, Bill Nelson, Amelia Philips and Christopher Steuart, course technology,5th Edition,2015 Additional
3) https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project 5)
4) https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10 6)
5) https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents 7)
6) https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_
7) Guide 8) https://cve.mitre.org/ 9) https://access.redhat.com/blogs/766093/posts/2914051 10)
8) http://resources.infosecinstitute.com/applications-threat-modeling/#gref 11)
9) http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Reference(s):

1) Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGrawHill,2nd Edition,2003
2) Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013