Year: B. Tech III (Semester VI)

Subject Name: Cyber Crime and Investigation Techniques **Subject Code:** BTEA19623
Type of course: Honors (Group: Cyber Security)
Prerequisite: Ethical Hacking and Penetration Testing

Rationale: This course explores technical, legal, and social issues related to cybercrime. Cybercrime is a broad term that includes offenses where a computer may be the target, crimes where a computer may be a tool used in the commission of an existing offense, and crimes where a computer may play a subsidiary role such as offering evidence for the commission of an offense. This course introduces fundamentals of malware and sets up a protected static and dynamic malware analysis environment. It teaches various malware behavior monitoring tools and actionable detection signatures from malware indicators.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
4	0	2	5	60	25	15	30	20	150

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No	Contents	Total Hrs
1.	**Cyber Crime:** Definition and Origin of the Word, Cyber Crime, and Information Security, who are Cyber Criminals, Classification of Cybercrimes, E-mail Spoofing, Spam Ming, Cyber Defamation, Internet Time Theft, Salami Attack, Salami technique Data Diddling, Forgery, Web Jacking, Newsgroup Spam, Industrial Spying, Hacking, Online Frauds, Pornographic Offenders, Software Piracy, Computer Sabotage Email Bombing, Computer Network Intrusion, Password Sniffing, Credit Card Frauds, Identity Theft	08
2.	**Cyber Offenses:** How Criminals plan them, Categories of Cyber Crimes, How Criminal Plans the Attack: Active Attacks, Passive Attacks, Social Engineering, Classification of Social Engineering, Cyber Stalking: types of Stalkers, Cyber Cafe and Cyber Crimes, Botnets, Attack Vectors, Cyber Crime and Cloud Computing	08
3.	**Cybercrime:** Mobile and Wireless Devices, Proliferation of Mobile and Wireless devices, Trends in Mobility, Credit card Frauds in Mobile and wireless devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organization Security policies and Measures in Mobile Computing Era	12

4.	**Tools and Methods used in Cybercrime:** Proxy server and Anonymizers, phishing: How Phishing works? How does password cracking work? Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Dos and DDos Attacks, SQL Injection, Buffer Overflow, An Attacks on Wireless Networks	**08**
5	**Introduction to Malware:** Introduction to Malware, OS security concepts, Malware threats, evolution of Malware, Malware types- viruses, worms, rootkits, Trojans, bots, spy-ware, adware, logic bombs, Malware analysis, Static Malware analysis, Dynamic Malware Analysis.	**08**
6	**Virtual Machines and Emulators:** Benefits Of Virtualization, Oracle Virtual Box, VMware Player, Virtual PC, Open-source Alternatives: Bochs, QEMU, KVM	**04**
7.	**Malware Functionality:** Down-loaders, Back-doors, Credential Stealer's Persistence Mechanisms, Privilege Escalation, Covert Malware launching Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection	**06**
8.	**Malware Detection Techniques:** Signature-based techniques: Malware signatures, packed Malware signature, metamorphic and polymorphic Malware signature non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences.	**06**

Suggested Specification table with Marks (Theory): (For B.Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
15	15	15	10	05	00

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr. No	Title of Book /Article	Author(s)	Publisher and details like ISBN	Year of publication /Publication Edition
1	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole and Sunit Belpure	Wiley	Latest Edition
2	Cyber Security and Cyber Laws	Alfred Basta, Nadine Basta, Mary Brown, Ravinder Kumar	Cengage	
3	Understanding cybercrime: Phenomena, challenges, and legal response	The International Telecommunication Union	The International Telecommunication Union	
4	Anti-Hacker Tool Kit	Mike Shema	McGraw Hill	

5	Practical malware analysis	Sikorski, Michael, and Andrew Honi	No Starch Press

Note: Students should refer to the latest editions of books

Course Outcomes (CO):

Sr. No	CO statements	Marks % weightage
CO-1	Identify and describe the major types of cybercrime.	30%
CO-2	Identify cybercrime vulnerabilities and exploitations of the Internet.	20%
CO-3	Analyze the various tools and methods used in cybercrime.	20%
CO-4	Explain the concept of secure operating system & virtualization and the nature of malware	20%
CO-5	Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.	10%

List of Open learning website:

- http://cybersecgroup.info/incident-response/cyber-incident-readiness-planning/malware-analysis-and-investigation
- https://www.csk.gov.in/

List of Open-Source Software:

- Kali Linux
- Wireshark
- SQLMap
- Bochs, QEMU, KVM
- IDA Pro
- OllyDbg, and WinDbg

List of Experiments:

Sr.No	Practical
	Case Study on Banking Fraud.

2.	Implementation of SQL injection so the query with attack parameters using SQL so the query with parameters.
3.	Using cross scripting with JavaScript programming so the vulnerability in any of the web page
4.	Set up a safe virtual environment to analyze Malware.
5.	Quickly extract network signatures and host-based indicators.
6.	Develop a methodology for unpacking Malware and get practical experience with five of the most popular packers.
7.	Using flooding techniques implement DDOS attacks.
8.	Demonstrate the use of password cracking tools.
9.	Demonstrate the use of keyloggers.
10.	Use key analysis tools like IDA Pro, OllyDbg, and WinDbg.