Year: B. Tech III (Semester VI)

Subject Name: Cyber Security and Cyber Law **Subject Code:**BTCO15602
Type of course: Open Elective -2
Prerequisite: NIL

Rationale: This course is of prime importance in Computer science and engineering. The knowledge inferred from huge amounts of historical data can be used for betterment of human lives in many ways. This course introduces the data pre-processing, various data mining methods and various applications of data mining.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
2	0	2	3	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

Contents:

Unit No	Contents	Total Hrs
1	**Introduction to Cyber Security :** Introduction, Computer Security, Threats, Harm, Vulnerabilities, Controls, Authentication, Access Control and Cryptography. **Web attack :** Browser Attacks, Web Attacks Targeting Users, Obtaining User or Website Data, Email Attacks. **Systems Vulnerability Scanning:** Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet	09
2	**Network Defense tools :** Network Defense tools Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Intrusion Detection System	06
3	**Web Application Tools :** Web Application Tools Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap.	06

	DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra	
4	**Cyber Crime and Cyber law :** Introduction to Cyber Crime and law Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Realms of the Cyber world, Recognizing and Defining Computer Crime, Contemporary Crimes, Contaminants and Destruction of Data, Indian IT ACT 2000	04
5	**Introduction to Cyber Crime Investigation :** Introduction to Cyber Crime Investigation Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless Networks.	05

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

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20	15	15	10	00	00

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

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

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 Paperback	Alfred Basta, Nadine Basta , Mary Brown, Ravinder Kumar	Cengage	2018
3	Anti-Hacker Tool Kit	Mike Shema	Mc Graw Hill.	

Course Outcomes (CO):

Sr. No.	CO statement	Marks % weightage
1	Understand Cyber Attack at System , network and Application level	30%
2	Identify various vulnerabilities through different scanners.	20%
3	Practice different steps to carry out Cyber attack using various open source tools.	10%
4	Differentiate between types of cyber crimes.	20%
5	Understand and examine Cyber Laws against various Cyber Crimes	10%
6	Utilize knowledge of this course to protect themselves and society against Cyber Attacks.	10%

List of Open learning website:
www.wireshark.org

List of Open Source Software

Nmap, , Zenmap, SQLMap, DVWA, Kali Linux

List of Experiments:

Sr.No	Practical
1	Study of basic Unix commands.
2	TCP/UDP connectivity using Netcat.
3	Perform Scan using Nmap.
4	Perform Scan using Zenmap.

5	Perform Network Scan using Wireshark.
6	To study SQLMAP
7	To Study DVWA for Web App Testing and manual SQL Injections.
8	XSS using DVWA.
9	Examine software keyloggers and hardware keyloggers.
10	Evaluate network defence tools for following (i) IP spoofing (ii) DOS attack
11	Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber-attack/vulnerability.
12	Perform online attacks and offline attacks of password cracking.