GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code: 3150714
Semester – V
Subject Name: Cyber Security

Type of course: Undergraduate (Open Elective)

Prerequisite: None

Rationale: In this digital age, the information and data are immense and need to be secured. The cyber crimes have increased as attackers see it as gaining big rewards. There is a need to examine the cyber attack patterns and provide security measures for them and also need to learn the cyber laws formed to effectively act upon cyber crimes.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
2	0	2	3	70	30	30	20	150

Content:

Sr. No.	Content	Total Hrs	Marks Weightage (%)
1	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	**08**	**25**
2	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: Introduction Detection System	**06**	**25**
3	Web Application Tools Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap. DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra	**06**	**25**
4	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.	**03**	**10**
5	Introduction to Cyber Crime Investigation Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer	**05**	**15**

	Overflow, Attack on wireless Networks.		

Suggested Specification table with Marks (Theory): (For BE only)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
20	**30**	**20**	**--**	**--**	**--**

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

Course Outcomes: Students will be able to

Sr. No.	CO statement	Marks % weightage
CO-1	Describe system and web vulnerability.	40
CO-2	Evaluate network defence tools.	30
CO-3	Understand the cyber laws	10
CO-4	Investigate a cybercrime, prepare report and apply laws for the case	20

Reference Books:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley
2. Cyber Security and Cyber Laws Paperback – 2018 by Alfred Basta, Nadine Basta , Mary Brown , Ravinder Kumar, publication Cengage
3. 3. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
4. Cyber security and laws – An Introduction, Madhumita Chaterjee, Sangita Chaudhary, Gaurav Sharma, Staredu Solutions

List of Open Source Software/learning website:
www.wireshark.org

List of Practical:

1. 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.
2. Evaluate network defense tools for following
   (i) IP spoofing
   (ii) DOS attack
3. Explore the Nmap tool and list how it can be used for network defence.
4. Explore the NetCat tool.
5. Use Wireshark tool and explore the packet format and content at each OSI layer.
6. Examine SQL injection attack.

7. Perform SQL injection with SQLMap on vulnerable website found using google dorks.

8. Examine software keyloggers and hardware keyloggers.
9. Perform online attacks and offline attacks of password cracking.
10. Consider a case study of cyber crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker..