Gyanmanjari Innovative University

Course Syllabus
Gyanmanjari College of Computer Application
Semester-5 (BCA)

Subject : Cyber security Fundamentals - BCACS10318

Type of course: Major Core

Prerequisite: Basic fundamental knowledge of computers, Internet and network

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
				SEE		CCE			
CI	T	P	C	Theory	Practical	MSE	LWA	ALA	
3	0	2	4	75	25	30	20	50	200

Legends: CI-Class Room Instructions; T – Tutorial; P - Practical; C – Credit; SEE - Semester End Evaluation; MSE- Mid Semester Examination; LWA - Lab Work Assessment; V – Viva voce; CCE-Continuous and Comprehensive Evaluation; ALA- Active Learning Activities.

Course Content:

Sr. No	Course content	Hrs	% Weightage
1	**Introduction to Cyber Security** • Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, CIA Triad, Assets and Threat, motive of attackers, Cyber Threats-Cyber Warfare, Networks Vulnerability Scanning - Netcat, Socat, understanding Port and	10	25%

	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		
2	**Network Defense tools** • Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, How a Firewall Protects a Network, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Introduction Detection System	10	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	10	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, Computer Language, Network Language, Realms of the Cyber world, A Brief History of the Internet, Recognizing and Defining Computer Crime, Contemporary Crimes, Computers as Targets, Contaminants and Destruction of Data, Indian IT ACT 2000.	6	10%
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	9	15%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Real-World Network Analysis:** Students will Analyze and make report on real-world Network Tool (Wireshark, Nmap,Snort, Traceroute)and upload it on GMIU Web Portal.	10
2	**Security Awareness:** Task students with creating posters, videos, or presentations to spread awareness about cyber threats.	10
3	**Evolution of Cyber Laws in India:** Research the evolution of cyber laws, focusing on the **Indian IT Act 2000** and its amendments. Compare Indian cyber laws with global standards and propose improvements and upload it on GMIU Web Portal.	10
4	**Cyber Crime Case Study :** Analyze real-life **cyber crime cases** (e.g., data breaches, credit card fraud). Prepare reports discussing the attack vector and applicable laws under the **IT Act 2000** and upload it on GMIU Web Portal.	10
5	**Password Cracking and Brute-Force Attacks :** Use tools like John the Ripper or THC-Hydra to perform online and offline password cracking. Test password strength and create reports on findings and upload it on GMIU Web Portal.	10
Total		50

Suggested Specification table with Marks (Theory):75

Distribution of Theory Marks **(Revised Bloom's Taxonomy)**						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage	25%	45%	15%	15%	0	0

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.

Course Outcome:

After learning the course the students should be able to:	
CO1	Understand core cyber security concepts, including threats, vulnerabilities, attack methods, tools for network scanning, reconnaissance, sniffing, injection.
CO2	Gain knowledge of firewalls, packet filtering, VPNs, NAT, intrusion detection systems, configuring security measures on Linux, Windows.
CO3	Identifying web vulnerabilities, inspecting applications, and cracking passwords with various tools and techniques.
CO4	Explore cybercrimes, attack strategies, digital forensics, incident response, and legal aspects, including the Indian IT Act 2000.
CO5	Develop skills to defend against cyber threats like malware, keyloggers, DoS/DDoS attacks, SQL injection, buffer overflow, and wireless network attacks.

List of Practical

Sr. No	Descriptions	Unit No	Hrs
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.	01	02
2	Evaluate network defense tools for following (i) IP spoofing (ii)DOS attack	01	02
3	Explore the Nmap tool and list how it can be used for network defence.	01	02
4	Port scanning using NMAP	01	02
5	Explore the NetCat tool.	01	02
6	TCP / UDP connectivity using Netcat	01	02
7	Use Wireshark tool and explore the packet format and content at each OSI layer.	02	02
8	Examine SQL injection attack.	03	02
9	Automated SQL injection with SqlMap	03	02
10	Perform SQL injection with SQLmap on vulnerable website found using google dorks.	03	02
11	Web application testing using DVWA	03	02
12	Manual SQL injection using DVWA	03	02
13	Examine software keyloggers and hardware keyloggers.	05	02
14	Perform online attacks and offline attacks of password cracking.	05	02

15	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..	05	02
		Total	30

Instructional Method:

The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory

The internal evaluation will be done on the basis of Active Learning Assignment

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

Reference Books:

[1] Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.

[2] Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley

[3] Cyber Security and Cyber Laws Paperback-2018 by Alfred Basta, Nadine Basta, Mary Brown, Ravinder Kumar, publication Cengage

[4] Cyber security and laws - An Introduction, Madhumita Chaterjee, Sangita Chaudhary, Gaurav Sharma, Staredu Solutions.