Gyanmanjari
Innovative University

Course Syllabus
Gyanmanjari College of Computer Application
Semester-6 (BCA)

Subject: Cyber Security Analysis and Reporting – BCACS10327

Type of course: Major Core

Prerequisite: Basic knowledge of Computer Networks, Operating Systems, and CyberSecurity Fundamentals and also possess analytical, problem-solving, and report-writing skills to analyze, handle, and document cyber incidents effectively.

Rationale:

This course equips students with the skills to analyze cyber threats, manage risks, and respond to security incidents effectively. It covers packet analysis, malware detection, email security, and incident handling through practical and theoretical learning. Students learn to evaluate vulnerabilities, apply risk management strategies, and document findings in professional reports. The unit prepares learners for real-world roles in cyber defense, digital forensics, and security operations.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
CI	T	P	C	SEE		CCE			
				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.*

3 Credits * 25 Marks = 75 Marks (each credit carries 25 Marks) Theory
1 Credits * 25 Marks = 25 Marks (each credit carries 25 Marks) Practical
SEE 100 Marks will be converted in to 50 Marks
CCE 100 Marks will be converted in to 50 Marks
It is compulsory to pass in each individual component.

Course Content:

Sr. No	Course content	Hrs	% Weightage
1	**Packet Analysis & Risk Management :** Introduction, Learning Objectives, Packet analysis and Packet Sniffers, Evaluating a packet sniffer, How packet sniffers work, The Multidisciplinary Approach, How to protect your sensitive resources? Frame the Threats and Sources, National Governments, Terrorists, Industrial Spies and Organized Crime Groups, Hacktivists, Hackers, Nature of the Computer Security Community, GAO Threat Table, Hierarchy of Needs, Multidisciplinary Risk Management, Solution strategies, Module 1 – Fundamentals of risk management, Module 2 – Applied standards and cyber risk management	10	20%
2	**Malware and Email Security Analysis :** Introduction, What is Malware Analysis, The Goals of Malware Analysis.Malware Analysis Techniques. Basic Static Analysis, Basic Dynamic Analysis, Threat and Vulnerability analysis of the email system.Threats:Spam, Social Engineering (phishing, targeted attacks), Massive eavesdropping, Other targeted criminal acts, Vulnerabilities: Integrity of email communications, Confidentiality of email communications,	10	20%
3	**Cyber Incident Handling :** The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist. Five Phases of Cyber security Incident Management: Plan & Prepare, Detect & Report, Assess & Decide, Respond & Post-Incident Activity. Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sources of Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization & Incident Notification.	8	20%
4	**Reporting and Documentation :** Types of reports – Executive, Technical, Forensic, Compliance, Structure of an incident report (summary, evidence, impact, recommendations) ,Report writing exercise with templates, Review of real-world security reports.	9	20%
5	**Wireless Network Analysis:** Wireless Networks, Wi-Fi Networks, Wireless Standards, WiFi Authentication Modes, Wireless Encryption, Wireless Threats, Wireless Hacking Methodology, Wireless Traffic Analysis.	8	20%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Email Encryption Demo :** Students are required to use tools such as GPG or ProtonMail to encrypt and decrypt email messages. They must submit screenshots of the process, explain the benefits of email encryption, and upload the completed work on the GMIU Web Portal.	10
2	**Identify and categorize threats :** Students are required to research a recent cybersecurity breach, categorize it according to the GAO Threat Table, and upload their findings on the GMIU Web Portal.	10
3	**Incident Report Writing :** Using standard templates, students create three structured reports on the same incident: an executive summary, a technical analysis, and a forensic report. They then upload these to the GMIU Web Portal.	10
4	**Breach News Analysis :** Pick a cyber breach that was covered in the media—like the Equifax or SolarWinds attacks. Your job is to write a short executive summary about it and then upload that summary to the GMIU Web Portal.	10
5	**Prepare Review Paper :** Students will prepare a review paper on a cybersecurity topic of your choice. You may work individually or in a group of four, under the guidance of a faculty advisor from the department. The final paper must be uploaded to the GMIU 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 and apply packet analysis and risk management techniques to identify and evaluate network threats.
CO2	Analyze malware and email security vulnerabilities using static and dynamic analysis methods to suggest preventive measures.
CO3	Demonstrate the ability to manage cybersecurity incidents through structured phases of detection, analysis, response, and recovery.
CO4	Prepare professional cybersecurity reports (executive, technical, forensic, and compliance) based on real-world scenarios and standardized templates.

List of Practical

Sr. No	Descriptions	Unit No	Hrs
1	1. Understand the concept of network packets and the need for packet analysis in cybersecurity. 2. Analyze TCP, UDP, and ICMP packets using Wireshark filters. 3. Evaluate Wireshark and Tcpdump as packet sniffers for accuracy and usability.	1	6
2	Frame the threats and identify possible sources affecting sensitive resources.	1	2
3	1. Create a customized GAO (Government Accountability Office) Threat Table. 2. Calculating Risk using Risk Assessment Matrix - Evaluate risk using Likelihood vs. Impact analysis. 3. Identify signs of port scanning, DoS patterns, and suspicious C2 traffic from pcap.	1	4
4	1. Capture HTTP traffic and reassemble files; observe TLS basics for HTTPS. 2. Identify signs of port scanning, DoS patterns, and suspicious C2 traffic from pcap.	1	4
5	Capture ARP and ICMP during network scans, simulate ARP spoof and show duplicated MACs.	1	2
6	Threat Analysis – Massive Eavesdropping Simulation - Demonstrate how unencrypted email communication can be intercepted.	2	2
7	Creating a Cyber Security Incident Response Checklist - Objective: Develop a standard checklist to guide the handling of security incidents.	3	2

8	Detecting Signs of an Incident and Observe warning signs of potential breaches (log anomalies, suspicious traffic, login failures).	3	2
9	1. Documenting Evidence and Analysis with Properly include logs, screenshots, or packet captures as evidence in reports. 2. Writing the Impact and Damage Assessment Section with Quantify and describe the operational, financial, or data loss impact of an incident.	4	4
10	**Consider of Case Study on :** 1. Insider Threat in a Software Company – Lessons in Incident Prevention and Handling 2. Supply Chain Ransomware Attack in 2025	4	2
	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 wili 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] Digital Forensics and Incident Response: Incident Detection and Investigation Using Digital Forensics Artifacts, Third Edition (2022), Gerard Johansen, Packt Publishing

[2] Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide, Second Edition (2012), Laura Chappell & Gerald Combs, Chappell University Press

[3] The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler, Second Edition (2011), Chris Eagle, No Starch Press

[4] The Practice of Network Security Monitoring: Understanding Incident Detection and Response, First Edition (2013), Richard Bejtlich, No Starch Press

[5] Network Forensics: Tracking Hackers Through Cyberspace by Sherri Davidoff & Jonathan Ham