GANPAT UNIVERSITY									
FACULTY OF ENGINEERING & TECHNOLOGY									
Programme	Bachelor of Technology					Branch/Spec.	Computer Science & Engineering (CBA-CS)		
Semester	VII					Version	1.0.0.0		
Effective from Academic Year			2022-23			Effective for the batch Admitted in			June 2021
Subject code	2CSE70E25		Subject Name			CYBER DEFENSE			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	1	0	4	Theory	40	60	100
Hours	3	0	2	0	5	Practical	30	20	50

Pre-requisites:

Web and OS security attack , computer network, network security

Learning Outcome:

After Successful completion of the course, students will be able to:

- Understanding cyber defense techniques
- Analyse log activity and incident of the threats
- Learn and apply threat detection techniques in live environment
- Understand different IT audit processes.

Theory syllabus

Unit	Content	Hrs
1	**Fundamentals of Cyber Defense**: Threat Landscape, Security Challenges, Defense Team, Information Security Control, Risk Level, Risk Management Cycle, CVSS scoring, NIST Framework	**9**
2	I**ncident Response Process** Incident response process: Reasons to have an IR process in place, Creating an incident response process, Incident response team, Incident life cycle, Handling an incident, Incident response in the cloud	**9**
3	**Security Audits** ISP-Information Security Policy, Creating, Enforcing ISP, Overview of audit, Network device audit, windows audit, linux audit, web server audit, database audit	**5**
4	**Log Analysis** Data correlation, Operating system logs, Firewall logs, Web server logs, Log Management Infrastructure,	**8**
5	**Detection Techniques** Honeypot Detection, Defending Against Fooling Attacks, Threats, Defending Against Denial of Service Attacks	**9**
6	**Implementing data recovery and disaster management** Disaster recovery plan: The disaster recovery planning process, Forming a disaster recovery team, Performing risk assessment, Prioritizing processes and operations, Determining recovery strategies, Creating the disaster recovery plan, Testing the plan, Obtaining approval, Maintaining the plan, Challenges	**5**

Suggested Practical List

Practical contents will be based on the Malware analysis, Cyber attack detection tchniques, Cyber attack prevention techniques, Log analysis and monitoring	
Text Books	
1	Data driven Security- Analysis, Visualization and dashboards by Jay Jacobs, Bob Rudis Wiley Publication.
Reference link	
1	Information Security and Auditing in the Digital Age: A Practical Managerial Perspective Amjad Umar
2	Cybersecurity: Attack and Defense Strategies: Infrastructure security with Red by by Erdal Ozkaya and Yuri Diogenes
3	Cyber Security Audit A Complete Guide - 2020 by Gerardus Blokdyk
4	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software By Michael Sikorski, Andrew Honig
5	Information Technology Control and Audit" by Angel R. Otero
Course Outcomes:	
COs	Description
CO1	Understanding defense techniques
CO2	Analyse log activity and incident of the threats
CO3	Learn and implement detection techniques in live environment
CO4	Understand different audit process

Mapping of CO and PO:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	0	1	1	2	1	1	2	0	1	0
CO2	3	2	3	3	3	2	3	3	2	1	1	1
CO3	3	2	1	2	3	2	2	3	2	1	2	1
CO4	3	2	3	2	2	2	3	3	3	2	2	2