JHARKHAND Rai University
RANCHI

End Semester/Reappear (Semester IV) Examination May 2025

Programme: BCA
Course: Cyber Security **Full Marks: 70**
Course Code:3CVAC203 **Time: 3 Hrs.**
Enrolment no. _____

Q. No.	Questions	CO	Bloom Taxonomy Category	Marks
	Section I			
1	**Short Answer type questions.**			**4 x 5 = 20**
a	1. Describe the cyber security traid in detail. Why CIA triad is important?	CO1	Understand	
	or			
	Define Crypto mining. How attackers use financial sector vulnerabilities to deploy crypto miners.	CO1	Understand	
b	Explain how DNS and VPN help protect enterprise networks from cyber threats	CO2	Understand	
	or			
	Summarize the main features of the MITRE ATT&CK framework.	CO2	Apply	
c	Illustrate three major cloud security challenges with real-world examples.	CO3	Apply	
	or			
	Discuss basic cloud security framework for a small enterprise.	CO3	Understand	
d	Describe the importance of Cloud security in cyber attacks.	CO3	Understand	
	or			
	What do you understand by Cloud computing and edge computing?	CO3	Analyze	
	Section II			
	Long Answer type questions.			**3 x 10 = 30**
2	Examine at least 4 network protection best practices using VPN and DNS.	CO4	Understand	
	or			
	Compare traditional IT infrastructure with cloud-based infrastructure in terms of security management?	CO4	Analyze	
3	Analyze the endpoint protection strategies to secure a smart home containing IoT devices like smart locks, cameras, and thermostats.	CO5	Analyze	
	or			
	What is an Incident Response Plan (IRP)? Describe its key phases.	CO5	Remember	
4	Explain the role of a SIEM platform in identifying and mitigating threats.	CO6	Understand	
	or			
	Illustrate the process of threat hunting and its significance in reducing cyber risks.	CO6	Apply	
	Section III			
	Application based questions			**1 x 20 = 20**
5	Evaluate the anatomy and impact of Insider Threat and Phishing cyber-attacks.	CO7	Evaluate	
	or			
	Examine the significance and advantages of setting up a Security Operations Center (SOC) within an organization. Additionally, analyze the difficulties SOC teams encounter when addressing advanced persistent threats (APTs).	CO7	Analyze	

Course Outcomes

CO1 Analyze top targeted industries and trends.
CO2 Explore how cyber criminals are using operating system tools to get control.
CO3 Uncover why cyber criminals are changing their techniques to gain illegal profits.
CO4 Determine what steps you can take to protect your organization against these threats.
CO5 Understand tools used by penetration testers and ethical hackers (network CLI tools, Telnet, SSH, Nmap, Wireshark, and many others).
CO6 Leverage high-end security enterprise solutions in high demand such as: IBM QRadar SIEM, Vulnerability Manager
CO7 Participate in Security Operation Center (SOC) role-playing scenarios