GOA UNIVERSITY

T.Y.BCA(NEP)(Semester -VI)
Subject Name: Cyber Security (Major)

Paper Title: Cyber Security **Paper Code:CSA-304**

Duration: 2:00 Hours **Total Marks:60**

Instructions: i)All questions are compulsory and figures to the right indicate full marks.
ii)Questions of 2 marks to be answered in not more than 40 words.
iii)Questions of 3 marks to be answered in not more than 60 words.
iv)Questions of 4 marks to be answered in not more than 80 words.
v) Questions of 5 marks to be answered in not more than 100 words.

Q.1 Answer the following questions: (6 x 2 = 12 marks)

i) What is the goal of cyber security?
ii) Define espionage in the context of cyber crime.
iii) What is a Trojan horse?
iv) List any two types of software piracy.
v) What is phishing?
vi) Name some commonly used tools in network forensics.

Q.2 A) i) What are the different types of Insider threats? (3) marks
ii) What is a quid pro quo attack? Give an example. (2) marks

OR

iii) Explain the significance of Stuxnet in cyber warfare. (3) marks
iv) What is a logic bomb? (2) marks

Q.2 B) i) What is the CIA Triad? Explain each component using examples. (5) marks
ii) What cyber security practices are made mandatory for financial institutions by RBI? (2) marks

Q.3 A) i) A suspect's laptop is handled by multiple forensic experts during an investigation. How would maintaining a chain of custody ensure the evidence is admissible? (3) marks

ii) A user's online account is at risk of unauthorized access. How would implementing multi-factor authentication improve the security of the account? (2) marks

X8Y2AA1E7X8Y2AA1E7X8Y2AA1E7X8Y2AA1E7

OR

	iii)	A system administrator notices that a user account can access another user's account by changing the URL parameters. Identify the type of privilege escalation and explain how it occurs.	(3) marks
	iv)	An organization wants to prevent unauthorized access to its systems. How can the principle of least privilege be applied?	(2) marks
Q.3B)	i)	During a cybercrime investigation, investigators examine network logs and identify the IP addresses used to access a system. Explain the importance of IP tracking.	(5) marks
	ii)	A cracker tries every possible password combination until the correct one is found. Explain this password cracking technique.	(2) marks
Q.4 A)	i)	Analyze how the DPDP Act helps protect users from misuse of their personal data.	(3) marks
	ii)	Identify the key steps in the vulnerability assessment process.	(2) marks

OR

	iii)	Analyze any three methods used to recover digital evidence.	(3) marks
	iv)	Explain how CSRF attacks exploit the trust between a user's browser and a web application.	(2) marks
Q.4B)	i)	Differentiate between white hat hackers and black hat hackers by analyzing their objectives, methods, and impact on cybersecurity.	(5) marks
	ii)	Examine the impact of an SQL injection attack.	(2) marks
Q.5 A)	i)	Evaluate the impact of cyber attacks on an e-commerce company.	(4) marks
	ii)	Explain the importance of enterprise security architecture in ethical hacking.	(2) marks

OR

	iii)	Compare and contrast the differences between active attacks and passive attacks.	(4) marks
	iv)	Evaluate the importance of email investigation.	(2) marks
Q.5B)	i)	A cyber attack targets a country's power grid system. Explain why critical infrastructure requires strong cybersecurity protection.	(3) marks
	ii)	A citizen becomes a victim of online identity theft. Which portal should they use to report the crime, and what is its role?	(3) marks

X8Y2AA1E7X8Y2AA1E7X8Y2AA1E7X8Y2AA1E7