Reg. No.															

Question Paper Code	13516

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Sixth Semester

B.Tech - Information Technology

20ITEL603 - CYBER SECURITY AND FORENSICS

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	What is the primary purpose of internet governance? (a) To control all internet content. (b) To establish policies and standards for the internet. (c) To monitor individual user activity. (d) To sell internet services.	1	K1	CO1
2.	Which of the following is a common challenge in internet governance? (a) Lack of available bandwidth. (b) Limited software updates. (c) Excessive hardware costs. (d) Difficulty in achieving global consensus.	1	K1	CO1
3.	Which of the following is a common challenge in internet governance? (a) Lack of available bandwidth. (b) Limited software updates. (c) Excessive hardware costs. (d) Difficulty in achieving global consensus.	1	K1	CO2
4.	Which of the following is a common challenge in data encryption? (a) Reduced hardware costs (b) Simplified software updates (c) Key management complexity (d) Improved network reliability	1	K1	CO2
5.	What is the primary goal of computer forensics? (a) To improve computer performance (b) To optimize network traffic (c) To enhance software development (d) To recover and analyze digital evidence	1	K1	CO3
6.	Why is a systematic approach crucial in computer investigations? (a) To increase processing speed (b) To simplify network design (c) To maintain the integrity of evidence (d) To reduce hardware costs	1	K1	CO3
7.	What is the significance of validating data acquisitions in ensuring evidence integrity? (a) To confuse and mislead attackers, diverting them from critical assets (b) To ensure that the acquired data is an exact copy of the original (c) To simplify software development (d) To improve hardware performance	1	K1	CO4
8.	How does contingency planning for image acquisitions prevent data loss? (a) By ignoring security risks (b) By having backup plans and procedures in case of errors or failures (c) By disabling all security measures (d) By promoting open access to data	1	K1	CO4
9.	What is the first step in processing a crime scene? (a) Analyzing data (b) Deleting evidence (c) Writing a report (d) Securing the scene	1	K1	CO5
10.	What is the purpose of validating forensics data? (a) To increase network speed (b) To encrypt data (c) To compress data (d) To ensure data integrity	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Summarize basic security measure for HTTP applications.	2	K2	CO1
12.	Illustrate vulnerability related to SOAP services.	2	K2	CO1
13.	Demonstrate a basic access control measure.	2	K2	CO2
14.	Explain the vulnerability of weak authentication.	2	K2	CO2
15.	Demonstrate a basic validation technique for acquired data.	2	K2	CO3
16.	List two storage formats for digital evidence.	2	K1	CO3
17.	Compare logical and physical data acquisition.	2	K2	CO4

18.	Interpret the use of remote network acquisition tools.		*2*	*K2*	*CO4*
19.	Demonstrate how to obtain a digital hash.		*2*	*K2*	*CO5*
20.	Outline the importance of validating forensics software.		*2*	*K2*	*CO5*
21.	Demonstrate how to use a network tool for traffic analysis.		*2*	*K2*	*CO6*
22.	Explain the importance of live acquisitions.		*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain the security vulnerabilities associated with SOAP services and differentiate them from those found in traditional HTTP applications. Relate these vulnerabilities to specific attack vectors.	*11*	*K2*	*CO1*
		OR			
	b)	Demonstrate the impact of notable security breaches on organizational reputation and financial stability. Justify the importance of proactive cyber security measures in mitigating these risks.	*11*	*K2*	*CO1*
24.	a)	Explain the vulnerabilities associated with open access to organizational data and weak authentication. Distinguish between different types of authentication methods and their effectiveness.	*11*	*K2*	*CO2*
		OR			
	b)	Demonstrate the effectiveness of GDPR in protecting personal data. Show the importance of data privacy regulations in the digital age.	*11*	*K2*	*CO2*
25.	a)	Illustrate a comprehensive procedure for conducting corporate high-tech investigations. Generate a plan for evidence preservation, analysis, and reporting.	*11*	*K2*	*CO3*
	b)	Compare and contrast the use of different forensic acquisition tools. Explain the significance of validating data acquisitions.	*11*	*K2*	*CO3*
26.	a)	Explain the factors that influence the determination of the best data acquisition method. Distinguish between logical and physical acquisitions and relate them to specific scenarios.	*11*	*K2*	*CO4*
		OR			
	b)	Interpret the effectiveness of contingency planning for image acquisitions. Summarize the need for backup procedures and alternative acquisition strategies.	*11*	*K2*	*CO4*
27.	a)	Construct the factors that influence the selection of appropriate computer forensics tools. Distinguish between hardware and software tools and relate them to specific investigation needs.	*11*	*K3*	*CO5*
		OR			
	b)	Develop the importance of validating and testing forensics software. Build the need for rigorous testing and quality assurance in digital forensics.	*11*	*K3*	*CO5*
28.	a)	Construct the techniques used in email investigations and cell phone/mobile device forensics. Distinguish between logical and physical acquisitions in mobile device forensics and relate them to specific evidence recovery scenarios.	*11*	*K3*	*CO6*
		OR			
	b)	Develop the importance of report writing in high-tech investigations. Identify the need for clear, concise, and accurate reports. Make use of forensic software tools in generating report findings.	*11*	*K3*	*CO6*