Reg. No.															

Question Paper Code	13976

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025

Seventh Semester

Computer Science and Engineering (Cyber Security)

20SCEL704 - IT SECURITY COMPLIANCE AND DIGITAL FORENSICS

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Non repudiation mainly prevents: a) Unauthorized access b) Denying a performed action later c) Data loss d) System crash	1	K1	CO1
2.	Policy enforcement is done via: a) Firewall rules b) Group Policy c) Access Control Lists d) All the above	1	K1	CO1
3.	Zero Trust architecture follows: a) Trust everyone inside network b) Trust no one c) Trust internal LAN only d) Trust perimeter firewall only	1	K1	CO2
4.	DMZ is mainly used to: a) Store DB Servers b) Keep Public Facing Servers c) Keep Backup Servers d) Keep Print Servers	1	K1	CO2
5.	Which protocol is recommended for secure data transmission over networks? a) FTP b) TLS c) Telnet d) HTTP	1	K1	CO3
6.	What is the primary role of a domain controller in server security? a) File sharing b) Authentication and authorization c) Print management d) Application deployment	1	K1	CO3
7.	Browser sandboxing helps to prevent: a) External access to OS resources b) Password reset c) SQL injection d) WAN routing	1	K1	CO4
8.	RAID is mainly used for: a) Fault Tolerance b) Encryption c) Authentication d) Routing	1	K1	CO4
9.	A key metric in an information security program is: a) Number of unauthorized access attempts detected c) Number of printers connected to the network c) Number of coffee breaks taken by staff d) Number of system reboots	1	K1	CO5
10.	Forensic lab standards mainly ensure: a) Low power usage b) Evidence validity + uniform process c) UI theme matching d) Lower storage cost	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Explain the purpose of the 'Availability' principle in information security.	2	K2	CO1
12.	Show the difference between LDAP and RADIUS authentication services.	2	K2	CO1
13.	Identify why network segmentation is considered a best practice for network security?	2	K2	CO2
14.	List out two protocols used for secure network transmission and briefly explain their purpose.	2	K2	CO2
15.	Give any two examples of secure configuration best practices.	2	K2	CO3
16.	Demonstrate the role of patch management in server security.	2	K2	CO3
17.	Compare full backup and an incremental backup.	2	K2	CO4
18.	Illustrate the importance of redundancy in disaster recovery.	2	K2	CO4
19.	Demonstrate how integration of security into an organization improves overall risk posture.	2	K2	CO5

20.	Interpret the term "principle of least privilege" and why is it important?		*2*	*K2*	*CO5*
21.	Outline the significance of log analysis in a forensic investigation.		*2*	*K2*	*CO6*
22.	Summarize why secure remote administration critical in maintaining system security?		*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Apply various threat categories and describe both technical and non technical countermeasures for each category.	*11*	*K3*	*CO1*
		OR			
	b)	Explain Authorization and Access control models in detail and compare implementation of access control in Windows & Unix with suitable diagrams.	*11*	*K3*	*CO1*
24.	a)	Discover the importance of network perimeters in modern network security architecture. How has the traditional perimeter model evolved with concepts like Zero Trust and cloud computing?	*11*	*K4*	*CO2*
		OR			
	b)	Analyze the security requirements for network traffic enterprise environment and explain the methods used for securing network transmission.	*11*	*K4*	*CO2*
25.	a)	Identify the function of data transmission protection protocols in server security. Provide descriptions of the mechanisms used to ensure confidentiality and integrity.	*11*	*K3*	*CO3*
		OR			
	b)	Organize the security implications and protection mechanisms for File, Print, and Application Servers hosted in hybrid and cloud environments.	*11*	*K3*	*CO3*
26.	a)	Analyze the layers of defense used to secure web and email applications, incorporating browser and endpoint controls. Justify how multi-layer reduces email attack success rate.	*11*	*K4*	*CO4*
		OR			
	b)	Examine the design considerations and best practices for building highly fault-tolerant, resilient IT systems in organizations with minimal downtime requirements.	*11*	*K4*	*CO4*
27.	a)	Discover the steps involved in developing an Information System Strategy in an organization, including risk based prioritization, technology alignment and governance integration.	*11*	*K4*	*CO5*
		OR			
	b)	Examine how organizations can effectively manage security compliance and perform audits in a dynamic regulatory environment and explain the role of digital compliance frameworks in shaping organizational security.	*11*	*K4*	*CO5*
28.	a)	Discuss the challenges involved in gathering and investigating evidence on a live system compared to a static system. Describe the procedures and tools used for live acquisition and the types of volatile data that must be captured.	*11*	*K3*	*CO6*
		OR			
	b)	Explain the role of Intrusion Detection Systems (IDS) and honeypots in network forensics and incident response.	*11*	*K3*	*CO6*