Reg. No.																

Question Paper Code	13937

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

Seventh Semester

Computer Science and Engineering

20CSEL708 - IT SECURITY COMPLIANCE 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.	LDAP stands for (a) Lightweight Directory Access Protocol (b) Long Directory Access Path (c) Local Directory Authentication Protocol (d) Linux Directory Application Protocol	*1*	*K1*	*CO1*
2.	Non-repudiation ensures (a) Availability of services (b) Users can deny their actions (c) Users cannot deny their actions (d) Confidential communication	*1*	*K1*	*CO1*
3.	What does a DMZ in network security refer to? (a) Internal encrypted area (b) Public guest network (c) De-Militarized Zone (d) Digital Masked Zone	*1*	*K1*	*CO2*
4.	What is the role of SSL in secure communications? (a) To increase speed (b) To filter spam (c) To authenticate and encrypt data (d) To assign IP addresses	*1*	*K1*	*CO2*
5.	Which server manages user authentication in a Windows network? (a) File Server (b) Domain Controller (c) Print Server (d) Web Server	*1*	*K1*	*CO3*
6.	DMARC is related to (a) DNS security (b) Email authentication (c) File sharing (d) Printing	*1*	*K1*	*CO3*
7.	Why is check pointing used? (a) Save system state for recovery (b) Encrypt backup data (c) Archive logs (d) Monitor bandwidth	*1*	*K1*	*CO4*
8.	Which backup type copies all files regardless of last changes? (a) Full backup (b) Incremental (c) Differential (d) Snapshot	*1*	*K1*	*CO4*
9.	Which of the following is NOT a security compliance standard? (a) ISO/IEC 27001 (b) HIPAA (c) PCI-DSS (d) HTML5	*1*	*K1*	*CO5*
10.	Which process ensures that all software remains up-to-date with the latest patches? (a) Logging (b) Updating (c) Auditing (d) Monitoring	*1*	*K1*	*CO6*

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Define confidentiality with an example.	*2*	*K1*	*CO1*
12.	State any two differences between authentication and authorization.	*2*	*K1*	*CO1*
13.	What is a firewall?	*2*	*K1*	*CO2*
14.	List any two encryption protocols used in data transmission.	*2*	*K1*	*CO2*
15.	Define server hardening with example.	*2*	*K1*	*CO3*
16.	Recall the advantages of using VPN.	*2*	*K1*	*CO3*
17.	Find any two advantages of cloud backup.	*2*	*K1*	*CO4*
18.	Differentiate between RTO and RPO.	*2*	*K2*	*CO4*
19.	Infer the term Information System Strategy.	*2*	*K2*	*CO5*
20.	Outline the link between disaster recovery and security compliance.	*2*	*K2*	*CO5*
21.	Define audit.	*2*	*K1*	*CO6*

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

22. Illustrate about secure remote administration. *2 K2 CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23. a) Discuss the components of the CIA triad in detail. *11 K2 CO1*

OR

b) Compare access control implementation in Windows and Unix environment. *11 K2 CO1*

24. a) Discuss any five common vulnerabilities found in computer network systems and their consequences. *11 K2 CO2*

OR

b) Illustrate the importance of analyzing traffic patterns for identifying security breaches. *11 K2 CO2*

25. a) Build the concept of baseline security. Develop the steps to secure different types of servers. *11 K3 CO3*

OR

b) Construct the methods of securing network infrastructure servers with examples. *11 K3 CO3*

26. a) Illustrate fault tolerance techniques in hardware and software. *11 K2 CO4*

OR

b) Interpret about hot backup and cold backup in a detailed manner. *11 K2 CO4*

27. a) Construct a basic auditing process for checking security policies in an organization. *11 K3 CO5*

OR

b) Build a simple plan to integrate security in an educational institution. *11 K3 CO5*

28. a) Examine a security architecture that uses honey pots and IDS for protecting a university network. *11 K4 CO6*

OR

b) Analyze the importance of managing updates and patch management with examples. *11 K4 CO6*