Reg. No															

B.Tech DEGREE EXAMINATION, MAY 2024

Fifth Semester

18CSE383T - INFORMATION ASSURANCE AND SECURITY

(For the candidates admitted during the academic year 2018-2019 to 2021-2022)

Note:

i. **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

ii. **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours **Max. Marks: 100**

PART - A (20 × 1 = 20 Marks)

Answer all Questions

		Marks	BL	CO
1.	____________________is the function of specifying access rights/privileges to the resources (A) Identification (B) Authentication (C) Authorization (D) Accountability	1	1	1
2.	Information should be consistently and readily accessible for authorized parties is called________________ (A) Availability (B) Integrity (C) Authentication (D) Confidentiality	1	1	1
3.	A hacker attempting to break into an information system is called ____________ (A) Intentional attack (B) Unintentional attack (C) Direct attack (D) Indirect attack	1	2	1
4.	A weakness or fault in a system or protection mechanism that opens it to attack or damage is called (A) Threat (B) Threat agent (C) Vulnerability (D) Attack	1	2	1
5.	A law that describes the violation of government laws enacted to protect the public is called________________ (A) Administrative law (B) Criminal law (C) Civil law (D) Intellectual Property Law	1	2	2
6.	A set of activities which focuses on short-term undertakings that will be completed within one or two years is said to be ______________ (A) Strategic planning (B) Tactical planning (C) Operational planning (D) Governance planning	1	2	2
7.	Which of the following is not a type of contingency planning? (A) Incident response plans (IRP) (B) Security Risk plans (SRP) (C) Disaster recovery plans (DRP) (D) Business continuity plans (BCP)	1	2	2
8.	____________ involves replacing each letter of the alphabet with the letter standing three places further down the alphabet (A) Monoalphabetic Ciphers (B) Caesar Cipher (C) Polyalphabetic Ciphers (D) One-Time Pad	1	2	2
9.	Choose the correct list of phases of Lewin change model from the following: (A) Moving – Unfreezing - Refreezing (B) Unfreezing – Moving – Refreezing (C) Unfreezing - Selecting – Refreezing (D) Selecting - Unfreezing – Refreezing	1	2	3

10. Which of the following is the role in senior management? 1 1 3

(A) Information Assurance Control Assessor
(B) Information System Owner
(C) Information Assurance Engineer
(D) Chief Security Officer

11. Which of the following is the correct sequence of activities in risk identification process? 1 2 3

(A) Identify, Inventory, and Categorize Assets , Plan and Organize the Process, Classify, Value, and Prioritize Information Assets , Identify and Prioritize Threats , Specify Asset Vulnerabilities
(B) Specify Asset Vulnerabilities , Plan and Organize the Process , Identify, Inventory, and Categorize Assets , Classify, Value, and Prioritize Information Assets , Identify and Prioritize Threats
(C) Identify and Prioritize Threats , Plan and Organize the Process , Identify, Inventory, and Categorize Assets , Classify, Value, and Prioritize Information Assets , Specify Asset Vulnerabilities
(D) Plan and Organize the Process, Identify, Inventory, and Categorize Assets , Classify, Value, and Prioritize Information Assets, Identify and Prioritize Threats , Specify Asset Vulnerabilities

12. __________ is a statement of principles, rules, and guidelines which the organization follows in order to achieve a desired outcome. 1 1 3

(A) Standards
(B) Policy
(C) Guidelines
(D) Procedures

13. Requirement analysis/ development, Risk assessment, Budgeting, Security planning, Security control development, and Security test and evaluation are the sub tasks of _______________ in Information Assurance in System Development Life Cycle. 1 2 4

(A) Initiation Phase
(B) Development/Acquisition Phase
(C) Implementation Phase
(D) Operation/Maintenance Phase

14. ________ can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system. 1 1 4

(A) System Acquisition
(B) Change Management
(C) Configuration Management
(D) System Development

15. _______________ is not a Preventive Information Assurance Tools? 1 2 4

(A) Gateway
(B) Cryptographic Protocols and Tools
(C) Firewalls
(D) Network Intrusion Prevention System

16. Which of the following statement is not true about Information assurance Awareness, Training, and Education (AT&E): 1 2 4

(A) An AT&E program raises an organization's reputation and brand
(B) An AT&E program maximizes the severity and number of information assurance Incidents
(C) An AT&E program provides better protection for assets
(D) An AT&E program reduces the risk of lawsuits against the organization

17. ___________ involves conducting reconnaissance scans against an organization's perimeter defenses such as routers, switches, firewalls, servers, and workstations to allow the organization to determine the overall network topology. 1 2 5

(A) System Testing
(B) Acceptance Testing
(C) Vulnerabilities Testing
(D) Penetration Testing

18. ________________ is a cybersecurity tool designed to broaden visibility into malware threats across networks, systems, and endpoints. 1 1 5

(A) Host-based scanners (B) Network-based scanners
(C) Malware analysis scanners (D) Distributed network scanners

19. A Network tool that captures copies of packets from network and analyzes them is called...... 1 1 5

(A) Packet Reader (B) Packet Sniffer
(C) Network Monitor (D) Port Scanner

20. ____________ tools provide access control to log information and enables system administrators to trace attacks or suspicious activities. 1 2 5

(A) Log management (B) Asset Management
(C) Risk Management (D) Access Management

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

Marks BL CO

21. State the implications on the Lack of Information Assurance? 4 1 1

22. Enlist on the different categories of Threats. 4 1 1

23. With suitable example, explain the Substitution Cipher and Transposition Cipher? 4 3 2

24. Illustrate in detail about Information Security Planning? 4 1 2

25. Information asset A is an online e-commerce database. Industry reports indicate a 10 percent chance of an attack this year, based on an estimate of one attack every 10 years. The information security and IT departments report that if the organization is attacked, the attack has a 50 percent chance of success based on current asset vulnerabilities and protection mechanisms. The asset is valued at a score of 50 on a scale of 0 to 100, and information security and IT staff expect that 100 percent of the asset would be lost or compromised by a successful attack. You estimate that the assumptions and data are 90 percent accurate. Calculate Risk. 4 4 3

26. Enlist the Benefits of Physical and Environmental Security Controls. 4 2 4

27. What is vulnerability scanner? Distinguish various vulnerability scanner in terms of its functionality. 4 4 5

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

Marks BL CO

28. (a) With neat diagram, elaborate the Security measures in System lifecycle in detail. 12 2 1

(OR)

(b) Illustrate with suitable example on how different types of software attacks work?

29. (a) Describe in details the various cryptographic tools used for secure communication. 12 3 2

(OR)

(b) What is policy in information assurance? Explain how to apply various types of policy in detail.

30. (a) Define risk management?With a neat sketch, elaborate on the risk management process. 12 2 3

(OR)

(b) Describe in detail about information security project management and discuss on the development of security project plan?

31. (a) Discuss in detail about the purpose, benefits, design, development and Assessment of Information Assurance Awareness, Training, and Education (AT & E). 12 2 4

(OR)

(b) Write a note on preventive Information assurance tools and discuss on the various preventive information assurance controls with suitable example.

32. (a) Illustrate with a detailed case study on Intrusion Detection and Prevention System (IDPS) 12 2 5

(OR)

(b) With suitable scenario, explain in detail about Information Assurance Measurement Process.

* * * * *