

Reg. No.														
----------	--	--	--	--	--	--	--	--	--	--	--	--	--	--

**B.Tech/ M.Tech (Integrated) DEGREE EXAMINATION, MAY 2024**  
Sixth Semester

**21CSE282T – INFORMATION SECURITY**

*(For the candidates admitted from the academic year 2022-2023 onwards)*

**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 40<sup>th</sup> minute.
- (ii) **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours

Max. Marks: 75

**PART – A (20 × 1 = 20Marks)**

Marks    BL    CO    PO

Answer **ALL** Questions

- |   |   |   |   |   |
|---|---|---|---|---|
| 1. _____ of information security is the quality of state of having ownership or control of some object or item.   | 1 | 3 | 1 | 2 |
| (A) Possession  |   |   |   |   |
| (B) Utility   |   |   |   |   |
| (C) Accuracy  |   |   |   |   |
| (D) Authorization   |   |   |   |   |
| 2. Which encompasses the protection of an organization's communications media, technology and content its ability use these tools to achieve the objective? | 1 | 2 | 1 | 2 |
| (A) Physical security   |   |   |   |   |
| (B) Communication security  |   |   |   |   |
| (C) Information security  |   |   |   |   |
| (D) Network security  |   |   |   |   |
| 3. MIS stands for _____.  | 1 | 2 | 1 | 2 |
| (A) Mail Integrity System   |   |   |   |   |
| (B) Mass Service System   |   |   |   |   |
| (C) Manager of Information System   |   |   |   |   |
| (D) Mail Security System  |   |   |   |   |
| 4. Compromising confidential information comes under which of the following category.   | 1 | 1 | 1 | 2 |
| (A) Bug   |   |   |   |   |
| (B) Threat  |   |   |   |   |
| (C) Virus   |   |   |   |   |
| (D) Attack  |   |   |   |   |
| 5. What type of attack a coordinated stream of request is launched against a target from many locations at the same time?                                   | 1 | 1 | 2 | 3 |
| (A) DDoS  |   |   |   |   |
| (B) Spoofing  |   |   |   |   |
| (C) Password attack   |   |   |   |   |
| (D) Man in the middle attack  |   |   |   |   |
| 6. SLA stands for _____.  | 1 | 2 | 2 | 2 |
| (A) Service Level Accuracy  |   |   |   |   |
| (B) Service Level Availability  |   |   |   |   |
| (C) Service Level Agreement   |   |   |   |   |
| (D) System Level Accuracy   |   |   |   |   |
| 7. Which method identified weakness in a collection of controlled system, where controls are not present or no longer effective                             | 1 | 2 | 2 | 2 |
| (A) Vulnerability   |   |   |   |   |
| (B) Threat  |   |   |   |   |
| (C) Spike   |   |   |   |   |
| (D) Surge   |   |   |   |   |

8. SNMP stands for \_\_\_\_\_. 1 3 2 2  
 (A) Simple Network Manager Protocol (B) Single Netsim Management Protocols  
 (C) Simple Netsim Manager Process (D) Simple Network Management Protocol
9. DRP stands for \_\_\_\_\_. 1 2 3 2  
 (A) Distribute Recovery Plan (B) Disaster Recovery Plan  
 (C) Disaster Reuse Plan (D) Disaster Recycle Plan
10. What is the formula for calculating cost benefit analysis? 1 2 3 2  
 (A)  $CBA = ALE (Prior) - ALE (Post) - ACS$  (B)  $CBA = ALE + ARO$   
 (C)  $CBA = SLE \times ARO$  (D)  $CBA = ACS - ALE$
11. Managed by a central authority in the organization can be based on individuals role is called \_\_\_\_\_. 1 3 3 2  
 (A) Non discretionary controls (B) Controlling risk  
 (C) Reduced risk (D) Delphi technique
12. When we have controlled any give vulnerability as much as we can, there is often risk that has not been completely removed or shifted reminder is called 1 1 3 2  
 (A) Controlling risk (B) Reduced risk  
 (C) Residual risk (D) Lattice based risk
13. SYSSP stands for \_\_\_\_\_. 1 2 4 3  
 (A) Software Secure Policy (B) System Specific Policy  
 (C) Software Security Policy (D) System Security Policy
14. \_\_\_\_\_ is the first level of security that protects all internal systems from outside threats. 1 2 4 2  
 (A) Firewall (B) Security perimeter  
 (C) Gateway router (D) Virus
15. \_\_\_\_\_ compresses a set of plane designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of operations. 1 4 4 3  
 (A) Business continuity plan (B) Incident plan  
 (C) Risk plan (D) Contingency planning
16. DMZ stands for \_\_\_\_\_. 1 3 4 3  
 (A) Divide Zone (B) Demilitarized Zone  
 (C) Demilit Zone (D) Deprocess Zone
17. \_\_\_\_\_ were created in response to the rising need to verify information system via electronic system. 1 4 5 2  
 (A) Digital signatures (B) Digital certificates  
 (C) Cryptography (D) Steganography

18. Collection of honey pots connecting several honey pot systems on a subnet is called \_\_\_\_\_.  
 (A) Honey nets (B) Honey pots  
 (C) Padded cell (D) Signatures

1 2 5 2

19. \_\_\_\_\_ monitors network traffic in real time for any intrusion.  
 (A) Host based ID's (B) Network based ID's  
 (C) Check point ID's (D) Firewall ID's

1 3 5 2

20. Digital signature cannot provide \_\_\_\_\_ for the message.  
 (A) Authentication (B) Non repudiation  
 (C) Integrity (D) Confidentiality

1 4 5 2

**PART – B (5 × 8 = 40 Marks)**

Marks BL CO PO

Answer **ALL** Questions

21. a. Discuss about NSITISSC security model in detail with suitable example.

8 2 1 2

**(OR)**

b. Explain about SDLC waterfall methodology and its relation in respect to information security.

8 2 1 2

22. a.i. Construct with the help of a table any four threats with its example

4 3 2 2

ii. Interpret the following terms: Macro virus and Boot virus.

4 3 2 2

**(OR)**

b. Develop the types of security policies in detail.

8 3 2 2

23. a. Explain the various steps involved in risk assessment with example.

8 2 3 2

**(OR)**

b. Explain with an example about the best practices followed in an organization.

8 2 3 2

24. a. Explain the goals used for design security architecture with the help of a diagram.

8 2 4 2

**(OR)**

b. How is IT different from routine management planning? What are the components of contingency planning?

8 2 4 3

25. a. What do you mean by cryptography? Discuss the authentication models used in cryptography.

8 2 5 2

**(OR)**

b. Write short notes on scanning and analysis tools used during the security design.

8 2 5 3

**PART – C (1 × 15 = 15 Marks)**

Answer ANY ONE Question

Marks BL CO PO

26. Design the purpose of Security Education Training and Awareness (SETA) given to employees. Explain the elements. 15 1 5 3
27. Construct, a small family owned company made extensive use of online banking and automated clearing house (ACH) transfers. Employee logged in which both a company and user specific ID card password. Two challenges questions had to be answered for transactions over ₹ 1500. The owner notified that an ACH transfer of ₹ 10,000 was initiated by an unknown source. They contacted the bank and identified, had made six transfers from the company bank accounts totaling ₹ 55,000. How? 15 5 2 3
- (i) What are the potential attacks justify your answer?
  - (ii) What lessons you can learn from this case study?
  - (iii) What is the impact and response in the above scenario?

\* \* \* \* \*