32. A. Elaborate in detail about the Intrusion Prevention and Intrusion Detection systems with precise examples. 12 2 5

(OR)

B. Identify and distinguish between the different types of malware and its detection methods.

* * * * *

Reg. No

B.Tech. DEGREE EXAMINATION, JUNE 2023

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

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

Part - A (20 × 1 Marks = 20 Marks)

Answer **All** Questions

Marks BL CO

1. Identify the true statement of security education, security training, and security awareness (SETA). 1 2 1
   (A) The purpose of SETA is to enhance security by Improving awareness, developing skills and knowledge and building in-depth knowledge
   (B) The purpose of SETA is to enhance security by Improving awareness, developing skills and knowledge and to maintain the system
   (C) The purpose of SETA is to enhance security by training and developing skills and knowledge and fix bugs
   (D) The purpose of SETA is to enhance security by fixing bugs, developing skills and risk management

2. SSCP stand for 1 1 1
   (A) Systems Scrutiny Certified Practitioner
   (B) Systems Sales Certified Practitioner
   (C) Systems Standard Centric Practitioner
   (D) Systems Security Certified Practitioner

3. Pick out the passive attack from the following 1 1 1
   (A) DDoS attack
   (B) Masquerade
   (C) Traffic Analysis
   (D) Phishing

4. Technical software failures or error is called as ____________. 1 1 1
   (A) Bugs, Code problems, unknown loopholes
   (B) Antiquated or outdated technologies
   (C) Equipment failure
   (D) Destruction of systems or information

5. Select the test that is performed on a computer system to evaluate its security 1 1 2
   (A) Penetration test
   (B) Alpha test
   (C) Beta Test
   (D) Quality test

6. BYOD stands for 1 1 2
   (A) Bring-Your-Own-Data
   (B) Bring-Your-Own-Device
   (C) Bring-Your-Original-Device
   (D) Bring-Your-Original-Data

7. "Social engineering attacks -wherein a user will be misled into revealing vital personal or critical information like system passwords to a source that disguises itself as legitimate". Identify the name of the attack 1 2 2
   (A) Social Engineering Attack
   (B) Man in the middle attack
   (C) Phishing
   (D) Snoofing

8. Phishing is a form of 1 1 2
   (A) Spamming
   (B) Scanning
   (C) Identify Theft
   (D) Impersonation

9. Identify the true statement about the information security policy. 1 3 3
I. Conveys management's intentions to its employees.
II. Set of guidelines or instructions
III. Organization's senior management implements idea
IV. Specifics and outline
(A) I only (B) II only
(C) I, II and III (D) II and IV only

10. Recognize the law that deals with the administration of a civil society (property and commercial). 1 2 3
(A) Administrative law (B) Public Law
(C) Tort Law (D) Patent

11. Select the key size of Monoalphabetic Cipher 1 1 3
(A) 52 (B) 26
(C) 72 (D) 62

12. Pick the correct equation that defines Expected loss per risk 1 1 3
(A) Annualized loss expectancy =Multiple loss expectancy *Annualized rate of occurrence
(B) Annualized loss expectancy = Single gain expectancy *Annualized rate of occurrence
(C) Annualized loss expectancy = Single loss expectancy *Annualized rate of profit
(D) Annualized loss expectancy = Single loss expectancy *Annualized rate of occurrence

13. Identify the procedure which ensures that every alarm works properly. 1 3 4
(A) Duress Alarm response (B) Security alarm response
(C) Updation alarm response (D) Frequency Alarm response

14. __________ helps to completely erase the information stored on the magnetic surface 1 1 4
(A) Eraser-electric (B) Eraser-Auto
(C) Degaussing (D) Decasting

15. Which of the following is done among the project members in order to make everyone aware of the job roles in the project 1 1 4
(A) Job Description Circulation (B) Job Rotation
(C) Job Delicacy (D) Job Announcements

16. Select the true statement about signature-based IDS 1 3 5
(A) It cannot work with an Intrusion Prevention System
(B) It only identifies known signatures
(C) It detects never-before-seen anomalies
(D) It works best in large enterprises.

17. ____________ is the act of gaining illegal access to a network resulting from an individual's continuous exploring of the Wi-Fi wireless networks via a laptop with a Wi-Fi feature enabled 1 1 5
(A) War Gaining (B) War Driving
(C) War Distraction (D) War Grunting

18. The systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation is termed as 1 2 5
(A) Risk mitigation (B) Penetration testing
(C) Vulnerability assessment (D) Risk Assessment

19. An unknown malware, one not previously identified can be detected through change detection is called 1 2 5
(A) One day attack (B) Zero day attack
(C) Man in the middle attack (D) Brute Force Attack

20. NVD stands for 1 1 5
(A) U.S. NIST's National Vulnerability Database
(B) U.S NIST's Notion Vulnerability Database
(C) U.S NIST's Navigational Vulnerability Database
(D) U.S NIST's Non-Identical Vulnerability Database

Part - B (5 × 4 Marks = 20 Marks)

Answer **any 5** Questions

Marks BL CO

21. Compare Software Development Life cycle and Sec Software Development Life cycle 4 4 1

22. List the different categories of threats with proper examples 4 2 1

23. Examine in detail about the following ciphers with example 4 4 2
a. Ceaser cipher
b. Mono alphabetic cipher

24. Write does the functions of Asset Performance Management Maturity Model (APM). 4 2 3

25. Write short note on Preventive Information Assurance tool 4 1 4

26. How incident handling process playing important role in security? 4 2 5

27. Discuss about the components and the issues of different Information Security Policy 4 2 5

Part - C (5 × 12 Marks = 60 Marks)

Answer **All** Questions

Marks BL CO

28. A. Describe the Security Services, Information States, and Countermeasures as defined by the MSR model in detail. 12 2 1

(OR)

B. Briefly outline the layered approach of Defense-in-Depth and discuss the components in each category in detail.

29. A. Illustrate the course of action that will be designed to help an organization respond effectively to a significant future incident, event or situation that may or may not happen. Explain with a professional example 12 2 2

(OR)

B. Explain about crisis management with suitable examples

30. A. Some aspects of the implementation process are technical in nature and deal with the application of technology, while others deal instead with the human interface to technical systems. Illustrate about the technical and non-technical aspects of implementing information security 12 3 3

(OR)

B. Explain about risk management in detail

31. A. Why information assurance is needed . Explain in detail about information assurance awareness, training, education and its benefits 12 3 4

(OR)

B. A web application is to be developed to implement a shopping cart. Only authenticated users can get the service. There are various phases in software development. In which phase , the security issues to be incorporated. Give your suggestions regarding the inclusion of security parameters in the development of software with proper justification.