CSC 306

B.Sc. VIth SEMESTER EXAMINATION, 2023-24

COMPUTER SCIENCE

(Cyber Security & Cyber Laws)

(CBCS Mode)

AFFIX PRESCRIBED
RUBBER STAMP

Date (तिथि) : ____________________

Paper ID
(To be filled in the
OMR Sheet)

5400

अनुक्रमांक (अंकों में) :
Roll No. (In Figures) : □□□□□□□□□□□□□□□

अनुक्रमांक (शब्दों में) : ____

Roll No. (In Words) : ____

Time : 1:30 Hrs.
समय : 1:30 घण्टे

Max. Marks : 75
अधिकतम अंक : 75

नोट : पुस्तिका में 50 प्रश्न दिये गये हैं, सभी प्रश्न करने होंगे। प्रत्येक प्रश्न 1.5 अंक का होगा।

Important Instructions :

1. The candidate will write his/her Roll Number only at the places provided for, i.e. on the cover page and on the OMR answer sheet at the end and nowhere else.
2. Immediately on receipt of the question booklet, the candidate should check up the booklet and ensure that it contains all the pages and that no question is missing. If the candidate finds any discrepancy in the question booklet, he/she should report the invigilator within 10 minutes of the issue of this booklet and a fresh question booklet without any discrepancy be obtained.

महत्वपूर्ण निर्देश :

1. अभ्यर्थी अपने अनुक्रमांक केवल उन्हीं स्थानों पर लिखेंगे जो इसके लिए दिये गये हैं, अर्थात् प्रश्न पुस्तिका के मुख्य पृष्ठ तथा साथ दिये गये ओ०एम०आर० उत्तर पत्र पर, तथा अन्यत्र कहीं नहीं लिखेंगे।
2. प्रश्न पुस्तिका मिलते ही अभ्यर्थी को जाँच करके सुनिश्चित कर लेना चाहिए कि इस पुस्तिका में पूरे पृष्ठ हैं और कोई प्रश्न छूटा तो नहीं है। यदि कोई विसंगति है तो प्रश्न पुस्तिका मिलने के 10 मिनट के भीतर ही कक्ष परिप्रेक्षक को सूचित करना चाहिए और बिना त्रुटि की दूसरी प्रश्न पुस्तिका प्राप्त कर लेना चाहिए।

1. Which of the following is a type of cyber attack ?
   (A) Phishing
   (B) SQL Injections
   (C) Password Attack
   (D) All of the above

2. Which of the following is not an advantage of cyber security ?
   (A) Makes the system slower
   (B) Minimizes computer freezing and crashes
   (C) Gives privacy to users
   (D) Protects system against viruses

3. Which of the following act violates cyber security ?
   (A) Exploit
   (B) Attack
   (C) Threat
   (D) Vulnerability

4. Which of the following actions compromise cyber security ?
   (A) Program
   (B) AES
   (C) Threat
   (D) Algorithm

5. Which of the following is defined as an attempt to harm, damage or cause threat to a system or network ?
   (A) Digital crime
   (B) Threats
   (C) System hijacking
   (D) Cyber Attack

6. IT security in any firm or organization is maintained and handled by______
   (A) Software Security Specialist
   (B) CEO of the organization
   (C) Security Auditor
   (D) IT Security Engineer

7. What is the existence of weakness in a system or network is known as ?

(A) Attack

(B) Exploit

(C) Vulnerability

(D) Threat

8. Which of the following is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information.

(A) MiTM attack

(B) Phishing attack

(C) Website attack

(D) DoS attack

9. Which of the following is the least strong security encryption standard ?

(A) WPA3

(B) WPA2

(C) WWW

(D) WEP

10. Which of the following is not a type of cyber crime?

(A) Data theft

(B) Forgery

(C) Damage to data and systems

(D) Installing antivirus for protection

11. Which of the following is not done by cyber criminals ?

(A) Unauthorized account access

(B) Mass attack using Trojans as botnets

(C) Email spoofing and spamming

(D) Report vulnerability in any system

12. In which year the Indian IT Act, 2000 got updated ?

(A) 2024

(B) 2008

(C) 1995

(D) 1999

13. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds ?

(A) Cracking or illegally hack into any system

(B) Putting antivirus into the victim

(C) Programming

(D) Rebooting the System

14. ________is the process or mechanism used for converting ordinary plain text into garbled non-human readable text & vice-versa.

(A) Malware Analysis

(B) Exploit writing

(C) Reverse engineering

(D) Cryptography

15. _________ is a means of storing & transmitting information in a specific format so that only those for whom it is planned can understand or process it.

(A) Scripting

(B) Cryptography

(C) Reverse engineering

(D) Exploit writing

16. When plain text is converted to unreadable format, it is termed as ______

(A) Rotten text

(B) Raw text

(C) Cipher-text

(D) Cipheen-text

17. Cryptographic algorithms are based on mathematical algorithms where these algorithms use _______ for a secure transformation of data.

(A) Secret key

(B) External programs

(C) Add-ons

(D) Secondary key

18. Cryptography can be divided into ______ types.

(A) 5

(B) 4

(C) 3

(D) 2

19. Data which is easily readable & understandable without any special algorithm or method is called ______

(A) Cipher-text

(B) Plain text

(C) Raw text

(D) Encrypted text

20. Plain text are also called ______

(A) Cipher-text

(B) Converted text

(C) Clear-text

(D) encrypted text

21. ______ is the art & Science of cracking the cipher-text without knowing the key.

(A) Cracking

(B) Cryptanalysis

(C) Key

(D) Malware

22. The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called ______

(A) Cryptanalysis

(B) Decryption

(C) Reverse engineering

(D) Encryption

23. The method of reverting the encrypted text which is known as cipher text to its original form i.e. plain text is known as ______

(A) Cryptanalysis

(B) Decryption

(C) Reverse engineering

(D) Encryption

24. ______ takes the plain text and the key as input for creating cipher-text.

(A) Key

(B) Algorithm

(C) Tuning Algorithm

(D) Encryption Algorithm

25. It is very important to block unknown, strange and ______ within the corporate network.

(A) Infected sites

(B) Programs

(C) Extra Files

(D) Important folders

26. __________ is the technique used in business organizations and firms to protect IT assets.

(A) Ethical hacking

(B) Unethical hacking

(C) Fixing bugs

(D) Internal data-breach

27. _________ is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.

(A) Email security

(B) Email hacking

(C) Email Forwarding

(D) Email Accepting

28. ________ is a famous technological medium for the spread of malware, facing problems of spam & phishing attacks.

(A) Cloud

(B) Pen drive

(C) Website

(D) Emil

29. Which of them is not a proper method for email security ?

(A) Use strong password

(B) Use email Encryption

(C) Spam filters and malware scanners

(D) Click on unknown links to explore

30. Unsolicited Bulk E-mails (UBI) are called ________

(A) SMS

(B) MMS

(C) Spam emails

(D) Malicious text

31. What is internet ?

(A) A single network

(B) A collection of unrelated computers

(C) Connection of local area networks

(D) Interconnection of wide area networks

32. To join the internet, the computer has to be connected to a ________

(A) Internet architecture board

(B) Internet society

(C) Internet service provider

(D) Different computer

33. Which of the following protocols is used in the internet?

(A) HTTP

(B) DHCP

(C) DNS

(D) All of these

34. ________ is the practice and precautions taken to protect valuable information from unauthorized access., recording, disclosure or destruction.

(A) Network Management

(B) Database Policy

(C) Information Security

(D) Physical Security

35. Spywares can be used to steal ________ from the attacker's browser.

(A) Browsing history

(B) Company details

(C) Plug-ins used

(D) File details

36. Collecting freely available information over the internet is an example of _____ type of information gathering.

(A) Active

(B) Passive

(C) Active & Passive

(D) Non-Passive

37. _______ is the protection of smart-phones, phablets, tablets, and other portable tech –devices, & the networks to which they connect to, from threats & bugs.

(A) OS Security

(B) Database Security

(C) Cloud Security

(D) Mobile security

38. Mobile security is also known as _______

(A) OS Security

(B) Wireless security

(C) Cloud Security

(D) Database Security

39. A small data file in the browser.

(A) Cookie

(B) Web Server

(C) FTP

(D) Database

40. Which of them is not an example of physical hacking?

(A) Walk –in using piggybacking

(B) Sneak-in

(C) Break-in and steal

(D) Phishing

41. Which of the following comes after scanning phase in ethical hacking ?

(A) Scanning

(B) Maintaining

(C) Restart

(D) Gaining access

42. When you use the word______ it means you are protecting your data from getting disclosed.

(A) Confidentiality

(B) Internet

(C) Attention

(D) Availability

43. _________ means the protection of data from modification by unknown users.

(A) Attention

(B) Integrity

(C) Availability

(D) None

44. What is Cyber Security ?

(A) Cyber Security provides security against malware

(B) Cyber Security provides security against cyber-terrorists

(C) Cyber Security protects a system from cyber attacks

(D) All of the mentioned

45. What does cyber security protect ?

(A) Cyber security protects criminals

(B) Cyber security protects internet- connected systems

(C) Cyber security protects hackers

(D) None of the mentioned

46. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks or their associated information?

(A) Cyber attack

(B) Computer security

(C) Cryptography

(D) Digital hacking

47. Which of the following is a type of cyber security ?

(A) Cloud Security

(B) Network Security

(C) Application Security

(D) All of the above

48. What are the features of cyber security ?

(A) Compliance

(B) Defense against internal threats

(C) Threat Prevention

(D) All of the above

49. Which of the following is an objective of network security?

(A) Confidentiality

(B) Integrity

(C) Availability

(D) All of the above

50. Which of the followings is not a cybercrime?

(A) Denial of Service

(B) Man in the Middle

(C) Malware

(D) AES

*****