No. of Printed Pages : 12

20907

Booklet Serial No. 284365

Reg. No. U 0 5 T V 2 2 C 0002

**V Semester All U.G. Courses Degree Examination, December/January- 2024-25**

**COMPUTER SCIENCE**

**Cyber Security (SEC)**

**(Repeater/Regular)**

**Time : 2 Hours** **Maximum Marks : 50**

***Instructions to Candidates:***

1. ***Check for complete printing of 50 questions.***
2. ***All questions are MCQs.***
3. ***Each question carries one mark.***

1. Check for complete printing of **50** questions.
2. The last page of the question paper may be used for rough work.
3. Each question has four multiple choice answer and choose the correct one.
4. Darken the appropriate circle with ball pen.
5. Damaging/overwriting using whitener on the **OMR** sheets are strictly prohibited.
6. No candidates will be allowed to leave the examination Hall till the end of the session and without handing over his/her answer sheet to the invigilator.
7. Candidates should ensure that the invigilator has verified all the entries and that the invigilator has affixed his/her signature in the space provided on the **OMR**.

**[P.T.O.**

1. Which of the following is considered an element of cyber security?
   A) Network security.
   B) Operational security.
   C) Application security.
   D) All of the above.

2. What is the internet infrastructure primarily used for?
   A) Data storage.
   B) Data transfer.
   C) Voice communication.
   D) Power generation.

3. The protocol is commonly used for sending emails in cyberspace _____
   A) HTTP
   B) SMTP
   C) VPN
   D) FTP

4. Malware stands for?
   A) Multipurpose software
   B) Malfunctioned software.
   C) Malicious software.
   D) Malfunctioning of security.

5. What is a firewall used for in cybersecurity?
   A) To protect against physical intruders.
   B) To filter network traffic and prevent unauthorized access.
   C) To provide electricity to devices.
   D) To cool down computer systems.

6. The primary function of a web browser _____
   A) To create websites.
   B) To host websites.
   C) To access and display web content.
   D) To manage database systems.

7. Total types of scanning in cyber security is?
   A) 1
   B) 2
   C) 3
   D) 4

8. What is the primary goal of cyber security?
   A) To prevent all cyber attacks.
   B) To minimize risk and protect against potential threats.
   C) To maximize internet speed.
   D) To ensure complete privacy online.

9. The organization is responsible for managing the allocation of IP addresses and domain names on the internet _____.
   A) ICANN.
   B) WHO.
   C) UNESCO.
   D) NSA

10. Choose the features which violate cyber security.
   A) Exploit.
   B) Attack.
   C) Compliance.
   D) None.

11. Which entity is primarily responsible for regulating cyberspace?
    A) Global corporations.
    B) International organizations.
    C) Individual countries.
    D) Non - profit organizations.

12. What is the primary objective of cybercrime against women and children?
    A) Financial gain.
    B) Gaining unauthorized access to computer systems.
    C) Causing emotional distress.
    D) Promoting cybersecurity awareness.

13. Identify the legal form of hacking.
    A) Cracking.
    B) Non - ethical hacking.
    C) Ethical hacking.
    D) Hacktivism.

14. The cyber law primarily deal with _____
    A) laws related to outer space.
    B) Criminal law
    C) Legal issues involving computer networks and the internet.
    D) Environmental regulations.

15. One of the characteristics of ransomware is?
    A) It steals sensitive information.
    B) It blocks access to a system/files until ransom paid.
    C) It spreads through physical media (USB drives).
    D) It only affects mobile devices.

16. What is the purpose of a host firewall?

A) To increase the risk of security breaches.

B) To monitor and control incoming and outgoing network traffic on a device.

C) To disable network connectivity.

D) To prevent the installation of security updates.

17. What is financial fraud?

A) Legal financial transactions.

B) Unintentional financial errors.

C) Intentional deceptive practices for financial gain.

D) Financial assistance for those in need.

18. What is a keylogger?

A) A physical device used to record keystrokes on a keyboard.

B) A software program that captures keystrokes on a computer or mobile device.

C) A type of malware that encrypts files and demands payment for decryption.

D) A form of encryption used to protect sensitive data.

19. Identify the first computer virus among the following.

A) Blaster.

B) Creeper.

C) Sasser.

D) Both B and C.

20. The legal framework that governs the use of electronic signatures and records in

A) Electronic transactions act.

B) Information technology act.

C) Electronic records act.

D) Cybersecurity and privacy act.

21. What is a "hashtag" used for in social media?
    A) To separate paragraphs.
    B) To categorize and link content.
    C) To mark the beginning of a post.
    D) To hide content from certain users.

22. What is social network primarily designed for?
    A) Sharing physical addresses.
    B) Playing video games.
    C) Connecting individuals and groups online.
    D) Buying and selling products.

23. The most important step in system hacking is:
    A) Cracking passwords.
    B) Covering tracks.
    C) Information gathering.
    D) None of the above.

24. The type of social media platform primarily focuses on sharing short, 140-character messages called "tweets" _____.
    A) Social networking sites.
    B) Microblogging platforms.
    C) Multimedia sharing platforms.
    D) Professional n/w sites.

25. What is a key concern regarding social media privacy.
    A) Excessive sharing of personal information
    B) Lack of internet connection.
    C) Limited access to social media platforms.
    D) Government surveillance.

26. Which one is considered to be a type of antivirus program?

A) Kasperkey.

B) Mcafee.

C) Quick heal.

D) All of the above.

27. The _____ of a network is assessed using response and transit times.

A) Longevity.

B) Performance.

C) Reliability.

D) Security.

28. The term describes the process of monitoring social media channels for mentions of a brand, product or keyword _____.

A) Social listening.

B) Social posting.

C) Social engagement.

D) Social networking.

29. What laws govern the posting of in appropriate content on social media?

A) Social media act.

B) Digital content regulation act.

C) There are no specific laws.

D) Internet privacy act.

30. Which of these describes an ongoing pursuit by an individual/group?

A) Stalking.

B) Identity theft.

C) Phishing.

D) Bulling.

31. What are the main components of E-Commerce?

A) Electronic devices and softwares.

B) Internet connection and web browsers.

C) Buyers, sellers, products and transactions.

D) Payment gateways and shopping carts.

32. State whether True or False : Data encryption is primarily used to ensure confidentiality.

A) True.

B) False.

C) Cannot be interpreted.

D) None.

33. Which of the following is not a threats of E-commerce?

A) Global reach.

B) Malware.

C) Phishing.

D) Data breaches.

34. CHAP stands for?

A) Challenge Hardware Authentication Protocols.

B) Circuit Hardware Authentication Protocols.

C) Challenge Handshake Authentication Protocols.

D) Circuit Handshake Authentication Protocols.

35. What are common threats to E-commerce?

A) Customer satisfaction.

B) Marketing strategies.

C) Competitive pricing.

D) Data breaches and cyber attacks.

36. Choose the phrase from the list below that best describes the initial stage of ethical hacking.

A) ARP poisoning.

B) DNS poisoning.

C) Foot printing.

D) Enumeration.

37. Which of the following is the components of digital payment?

A) Point - of - sale.

B) Payment gateway.

C) Mobile wallets.

D) All of these.

38. Which of the following is **NOT** a mode of digital payment?

A) Banking cards.

B) Unified payment interface (UPI).

C) Physical currency.

D) e-wallets.

39. In which category does compromising confidential information fall?

A) Bug.

B) Threat.

C) Attack.

D) Vulnerability.

40. Which of the following tool is used in wi-fi hacking?

A) Aircrack-ng.

B) Wireshark.

C) Norton.

D) None.

41. USSD stands for :

A) User sale service data.

B) User supplementary service data.

C) Unstructured supplementary service data.

D) Unique supplementary service data.

42. They are malicious hackers whose primary goal is to commit cybercrimes to make money. Who are "they" in this context?

A) White hat hackers.

B) Black hat hackers.

C) Hacktivisits

D) Gray hat hackers

43. Which mode of digital payment involves using a plastic card issued by a bank to make transactions.

A) Unified payment interface (UPI).

B) E-wallets.

C) Banking cards.

D) USSD.

44. Choose among the following techniques, which are used to hide information inside a picture.

A) Image rendering.

B) Steganography

C) Rootkits.

D) Bitmapping.

45. How often should security patches be applied?

A) Once a year

B) Once a month.

C) Every 6 months.

D) As soon as they become available.

46. What is the recommended length for a strong password?
A) 4 characters.
B) 8 characters.
C) 16 characters.
D) 12 characters or more.

47. Determine the earliest method of free phone calls used by hackers.
A) Cracking.
B) Spamming.
C) Phreaking.
D) Phishing

48. Why is it important to keep third - party software upto date?
A) To increase system performance.
B) To reduce the risk of security vulnerabilities.
C) To limit the functionality of the software.
D) To make the software incompatible with other programs.

49. Which protocol is mostly used in wi-fi security?
A) WPS.
B) WPA
C) WPA2.
D) Both B and C.

50. Which of the following is **NOT** a common wi-fi security protocol?
A) WPA
B) WEPP.
C) WPA2.
D) SSL.