Roll. No. .....

O.M.R. Serial No. | | | | | | | | |

Question Booklet Number
603024

B.C.A. (SEM.-VI) (NEP) EXAMINATION, 2024

COMPUTER APPLICATION

(Information & Cyber Security)

[BCA-6001]

Paper Code							
Z	2	0	0	0	6	5	T

Question Booklet Series
D

Time : 1 : 30 Hours **Max. Marks : 75**

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 100 questions. Examinee is required to answer 75 questions in the OMR Answer-Sheet provided and not in the question booklet. All questions carry equal marks.
3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.
4. Four alternative answers are mentioned for each question as - A, B, C & D in the booklet. The candidate has to choose the correct / answer and mark the same in the OMR Answer-Sheet as per the direction :

(Remaining instructions on last page)

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 100 प्रश्न हैं। परीक्षार्थी को 75 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, प्रश्न-पुस्तिका पर नहीं। सभी प्रश्नों के अंक समान हैं।
3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गए हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, उसे तुरन्त बदल लें।
4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर- A, B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छाँटना है। उत्तर को OMR उत्तर-पत्रक में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

(शेष निर्देश अन्तिम पृष्ठ पर)

1. What is Digital Forensics?
   (A) Process of using scientific knowledge in analysis and presentation of evidence in court
   (B) The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, a chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation
   (C) A process where we develop and test hypotheses that answer questions about digital events
   (D) Use of science or technology in the investigation and establishment of the facts or evidence in a court of law

2. Which type of digital evidence can be extracted from volatile memory?
   (A) Deleted files
   (B) Browser history
   (C) Running processes and network connections
   (D) Encrypted data

3. Which World organization accredited labs in the world of forensics?
   (A) AKULD
   (B) APIOS
   (C) ACSLD
   (D) None of these

4. Which of the following is a commonly used forensic tool in digital investigations?
   (A) Photoshop
   (B) Wireshark
   (C) EnCase
   (D) Microsoft Office

5. What is the purpose of a hash value in digital forensics?
   (A) To encrypt sensitive data
   (B) To identify and verify the integrity of digital evidence
   (C) To recover deleted files from storage media
   (D) To analyze network traffic and detect malicious activities

6. What is the purpose of a write blocker in digital forensics?
   (A) To prevent unauthorized access to digital devices
   (B) To recover deleted data from storage media
   (C) To ensure that evidence is not altered during the investigation
   (D) To encrypt sensitive data for secure storage

7. What is the importance of chain of custody in digital forensics?
   (A) To ensure the admissibility of digital evidence in court
   (B) To prevent unauthorized access to digital devices
   (C) To track the physical movement and handling of digital evidence
   (D) To encrypt sensitive data for secure storage

8. 802.11i's final form is known as :

(A) Wi-Fi Protected Access

(B) Wired Equivalency Privacy

(C) Robust Security Network

(D) Both (A) and (B)

9. Central node of 802.11 wireless operations is _____

(A) Access Point

(B) WPA

(C) Access Port

(D) WAP

10. Penetration testing is used to :

(A) identify vulnerabilities and weaknesses

(B) address security flaws before malicious hackers exploit them

(C) Both (A) and (B)

(D) crash the site/system

11. Which of the following are ways to conduct penetration testing?

(A) Black Box Testing, White Box Testing, Grey Box Testing

(B) White Box Testing, Brown Box Testing, Red Box Testing

(C) Black Box Testing, Red Box Testing, Grey Box Testing

(D) Black Box Testing, Green Box Testing, White Box Testing

12. Black box and white box pentest is done from _____ and _____ user perspective respectively

(A) Insider; outsider

(B) Outsider; insider,

(C) Third party; insider

(D) Employee and user

13. Which of the following groups must a penetration testing result review?

(A) Documentation, Log, System Configuration, Ruleset, Network Sniffing, File Integrity

(B) Documentation, Log, System Configuration, Network Sniffing, File Integrity

(C) Documentation, Log, System Configuration, Network Sniffing, Ruleset, File Integrity, Personnel

(D) None of the above

14. What is the risk involved in doing penetration testing?

(A) Some operations of the company might slow down

(B) Skynet takes over the world

(C) VPN not effective

(D) Security is an issue

15. PKI stands for?

(A) Public Key Infrastructure

(B) Private Key Infrastructure

(C) Public Key Instance

(D) Private Key Instance

16. The digital signature can be suspended by the certifying authority in case of :
(A) public interest
(B) interest of user
(C) interest of any person
(D) Both (A) and (C)

17. Which among the following was established under IT Act, 2000 to resolve disputes arising from the law?
(A) Cyber Appellate Tribunal
(B) Technology Disputes Bureau
(C) Cyber Administrative Tribunal
(D) IT Disputes Tribunal

18. A major amendment to Information Technology Act, 2000 was made in which year?
(A) 2001
(B) 2016
(C) 2012
(D) 2008

19. Malware that Encrypts Files and Demands Payment is :
(A) Spyware
(B) Ransomware
(C) Adware
(D) Rootkit

20. Which type of malware is designed to observe and gather user information without their knowledge?
(A) Worm
(B) Trojan
(C) Spyware
(D) Adware

21. Harassing someone through electronic message is offence of :
(A) Hacking
(B) Squatting
(C) Stalking
(D) Phishing

22. In a phishing attack, what is the common method used to trick users into revealing sensitive information?
(A) Distributing malware-infected files
(B) Impersonating a trusted entity
(C) Launching DDoS attacks
(D) Encrypting files for ransom

23. _____ is a criminal offense of receiving money, property or services from a person, entity or institution, through coercion.
(A) Phishing
(B) Pornography
(C) Net or Cyber Extortion
(D) Credit Card Fraud

24. Smartphone penetration framework was devised by :
(A) Georgia Weidman ,Bulb Security LLC in 2014
(B) Georgia schoof by Dagah
(C) Georgia Weidman ,Bulb Security LLC in 2018
(D) Sergia Drapa

25. Password cracker tries :

(A) DOS attack

(B) Brute force attack

(C) Intrusion detection

(D) Intrusion prevention

26. Script kiddies are :

(A) Individuals who want to break into computers to create damage, yet lack the advanced knowledge of computers and networks needed to do so

(B) Individuals doing Ethical hacking

(C) Penetration tester

(D) Vulnerability assessor

27. First phase of hacking is :

(A) Maintaining access

(B) Gaining access

(C) Reconnaissance

(D) Scanning

28. What is the most important difference between ethical hacker and cracker ?

(A) The ethical hacker has authorization from the owner of the target

(B) The ethical hacker is just a cracker who is getting paid

(C) The ethical hacker does not use the same techniques or skills as a cracker

(D) The ethical hacker does it strictly for financial motives unlike a cracker

29. What type of hacker impose maximum threat to an organization ?

(A) Black-hat hackers

(B) Grey-hat hackers

(C) Script kiddies

(D) Disgruntled employees

30. Examples of hash functions are :

(A) MD5

(B) SHA-1

(C) Both (A) and (B)

(D) None of the above

31. Hash function is used in implementing ____ service of network security.

(A) Availability

(B) Integrity

(C) Confidentiality

(D) All of the above

32. Wireless LAN security architechture is defined in :

(A) IEEE 802.11

(B) IEEE 800.1

(C) IEEE802.11i

(D) Both (A) and (C)

33. Which of the following tool is used in Wi-Fi hacking ?

(A) Air Crack-ng

(B) Wireshark

(C) Norton

(D) None of the above

34. The Information Technology Act, 2000 come into force on :

(A) 9th June, 2000

(B) 17th October, 2000

(C) 15th December, 2000

(D) None of these

35. The key of a pair used to create a digital signature is known as :

(A) public key receiver

(B) private key of sender

(C) creator key

(D) secret key

36. The key of a key pair used to verify a digital signature :

(A) public key of sender

(B) private key sender

(C) verifying key

(D) secret key

37. An adjudicating officer, under the IT Act, 2000, for holding inquiry and imposing penalty is appointed by the :

(A) Controller

(B) Central Government

(C) Cyber Appellate Tribunal

(D) High Court

38. _____ is the unique value for message or content by applying strong Hash function.

(A) Decryption

(B) Encryption

(C) Message digest

(D) Private key

39. For ethical hacking, what process is followed :

(A) Cryptography

(B) Encryption

(C) Decryption

(D) Penetration Testing

40. What are the difficulties in handling Digital Evidence?

(A) Easy to destroy

(B) Easy to sustain

(C) Hard to get

(D) Both (A) and (C)

41. What is the Primary Objective of Digital Forensic for Business and Industry ?

(A) Availability of service

(B) Continuity of operation

(C) Prosecution

(D) Security

42. How does ISO/IEC 27000 define an 'asset' in relation to ISO/IEC 27001?

(A) Anything that is of value to the organisation

(B) A physical item within the organisation

(C) Digital and physical items owned by an organisation

(D) Tangible and non-tangible items owned or rented by an organisation

43. Annex A of ISO/IEC 27001 contains best practices for managing and securing information assets within an organisation. Which of the below are ISO 27001 control sets, as outlined in Annex A?

(A) Information security policies

(B) Asset management

(C) Access control

(D) All of the above

44. Which of the below are current threats to many organisations?

(A) Fraud

(B) Loss of information

(C) Unauthorised access

(D) All of the above

45. When should organisations perform an information security risk assessments?

(A) Monthly

(B) Every six months or when significant changes are proposed to occur

(C) Every 12 months, or when significant changes are proposed to occur

(D) At planned intervals or when significant changes are proposed to occur

46. As per ISO27001, who shall review the organisation's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness?

(A) External Auditor

(B) Internal Auditor - Your answer - you got this wrong

(C) Quality Manager

(D) Top Management

47. Within ISO standards, what does 'shall' indicate?

(A) A recommendation

(B) A permission

(C) A capability

(D) A requirement

48. Within ISO/IEC 27001, which clause relates to leadership and the role of top management in the establishment, implementation, maintenance, and continual improvement of the ISMS?

(A) 4

(B) 5

(C) 6

(D) 7

49. What is the goal of a backup and recovery strategy in disaster recovery planning?

(A) To eliminate all vulnerabilities

(B) To promote unrestricted data sharing

(C) To ensure the availability of data in case of a loss or compromise

(D) To ignore potential risks

50. What is the goal of a recovery strategy in disaster recovery planning?

(A) To eliminate all vulnerabilities

(B) To promote unrestricted data sharing

(C) To identify and prioritize recovery tasks and resources

(D) To ignore potential risks

51. The things Carried out by means of electronic data interchange, and other means of electronic communication is commonly referred to as :

(A) e-communication

(B) e- governance

(C) e- record

(D) e-commerce

52. The authentication to be affected by use of asymmetric crypto system and hash function is known as :

(A) Public key

(B) Private Key

(C) Digital Signature

(D) e- governance

53. The Central Government may appoint a _____ of Certifying Authority who shall exercise supervision over the activities of Certifying Authorities.

(A) Commissioner

(B) Controller

(C) Executive

(D) President

54. _____ is a person in whose name the Digital Signature Certificate is issued.

(A) Certified authority

(B) Subscriber

(C) Holder

(D) Controller

55. The _____ has the power to suspend or revoke Digital Signature Certificate.

(A) Commissioner

(B) Certifying Authority

(C) Subscriber

(D) Controller

56. Digital signatures created and verified using:

(A) Program

(B) Graphical coding

(C) HTML

(D) Cryptography

57. Which of the following refers to the violation of the principle if informationcomputer is no more accessible?

(A) Availability

(B) Confidentiality

(C) Access control

(D) All of the above

58. Which of the following provides legal framework for e-governance in India ?

(A) IT (Amendment) Act, 2008

(B) Indian Penal Code

(C) IT Act, 2000

(D) None of the above

59. Cyberspace has :

(A) No national boundaries

(B) International jurisdiction

(C) Limited boundaries

(D) Both (A) and (B)

60. Out of following which is the main authority is at the top and its main function is to issue license to the certifying authority and to supervise his functions ?

(A) Controller of certifying authority

(B) Verification authority

(C) Subscriber

(D) None of the above

61. _____ means a system of a secure key pair consisting of a private key for creating digital signature and public key for verifying digital signature.

(A) Asymmetric Cryptography

(B) Cryptosystem

(C) Symmetric cryptosystem

(D) None of the above

62. Public key cryptography is same as :

(A) Private key cryptography

(B) Asymmetric cryptography

(C) Symmetric cryptography

(D) Session key cryptography

63. Hash function are used for (encryption):

(A) Encryption

(B) Decryption

(C) Digital signature

(D) None of the above

64. Under Information Technology Act the purpose of digital signature is to :

(A) Forge the document

(B) Photocopy the document

(C) Digital Printing

(D) Ensure integrity

65. _____ Monitors all internet and other network activity, looking for suspicious data and preventing unauthorized access.

(A) Intrusion detection system

(B) Firewall

(C) Data encryption

(D) None of the above

66. Which of the following is an example of web application vulnerability ?

(A) Sql Injection

(B) DNS Spoofing

(C) Buffer Overflow

(D) Cross Site Scripting (XSS)

67. Under which section of information act 2000 amended in 2008 , stealing any digital asset or info is considered as a cyber crime ?

(A) 64

(B) 65

(C) 66

(D) 67

68. Public key of sender is used in encryption and private key of sender is used for decryption to ensure :

(A) Authentication

(B) Confidentiality

(C) Non-repudiation

(D) Availaibility

69. In Wi-Fi Security, which of the following protocol is more used?

(A) WPA

(B) WPA2

(C) WPS

(D) Both (A) and (C)

70. The transmitted message must make sense only to intended _____, in message confidentiality.

(A) Sender

(B) Receiver

(C) Translator

(D) Modulor

71. Hash functions guarantee message integrity and that the message has not been _____.

(A) Over view

(B) Replaced

(C) Violated

(D) Changed

72. Data must arrive exactly as it was sent to receiver from sender, is called _____.

(A) Message Sending

(B) Message Splashing

(C) Message Integrity

(D) Message Confidentiality

73. Wi-Fi is abbreviated as :

(A) Wireless FLAN

(B) Wireless LAN

(C) Wireless Fidelity

(D) Wired fellow

74. When there is an intermediate between the communications without the knowledge of the communicators, which type of threats is this?

(A) Network Injection

(B) Malicious Association

(C) Accidental Association

(D) Man in the middle attack

75. In which layer frequency band is defined and wireless signals are encoded?

(A) Medium Access Layer

(B) Physical Layer

(C) Logic Link Control Layer

(D) Both (B) and (C)

76. A communication is said to be insecure where data is transmitted in a manner that allows for interception also called?

(A) Attack

(B) Sniffing

(C) ISP

(D) Citation

77. The key of key pair used to create digital signature is called :

(A) Public key

(B) Private key

(C) Session key

(D) Secret key

78. The key pair of _____is used for creation and verification of digital signature.

(A) Sender

(B) Receiver

(C) Any of the above

(D) None of the above

79. Digital signature certificate is issued by (as in IT act 2000) :

(A) Appellate tribunal

(B) Controller of certificate authority

(C) Certificate authority

(D) Cyber crime investigator

80. e-governance include :

(A) Filing of form online, paperless

(B) Efficient , low cost, transparent governance

(C) Both (A) and (B)

(D) Payment of bills

81 Digital signature is defined under ____ section of IT Act,2000.

(A) Section 1

(B) Section 2

(C) Section 8

(D) Section 6

82. Information Technology Act, 2000 directed the formation of a Controller of Certifying Authorities to regulate the issuance of ____.

(A) Data license

(B) IP address in India

(C) Digital signatures

(D) Internet service provider license

83. Which of the following are the types of scanning?

(A) Network, vulnerability, and port scanning

(B) Port, network, and services

(C) Client, Server, and network

(D) None of the above

84. Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system?

(A) DDoS and Derive-by Downloads

(B) Malware and Malvertising

(C) Phishing and Password attacks

(D) All of the above

85. Password cracker tries :

(A) Man in the middle attack

(B) Brute force attack

(C) Intrusion detection

(D) Intrusion prevention

86. What is the primary goal of ethical hacker ?

(A) Avoiding detection

(B) Testing security controls

(C) Resolving security vulnerabilities

(D) Determining return on investment for security measures

87. Which one of the following refers to the technique used for verifying the integrity of the message?

(A) Digital signature

(B) Decryption algorithm

(C) Protocol

(D) Message Digest

88. Which one of the following is a type of antivirus program?

(A) Quick heal

(B) McAfee

(C) Kaspersky

(D) All of the above

89. In system hacking, which of the following is the most crucial activity?

(A) Information gathering

(B) Covering tracks

(C) Cracking passwords

(D) None of the above

90. To protect the computer system against the hacker and different kind of viruses, one must always keep _____ on in the computer system.

(A) Antivirus

(B) Firewall

(C) Vlc player

(D) Script

91. Which of the following are the types of scanning?

(A) Network, vulnerability, and port scanning

(B) Port, network, and services

(C) Client, aerver, and network

(D) None of the above

92. Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system ?

(A) DDoS and Derive-by Downloads

(B) Malware and Malvertising

(C) Phishing and Password attacks

(D) All of the above

93. Which type of the following malware does not replicate or clone them self's through infection?

(A) Rootkits

(B) Trojans

(C) Worms

(D) Viruses

94. What is the primary goal of a risk assessment in cybersecurity?

(A) To eliminate all cyber threats

(B) To identify and manage potential risks

(C) To promote unrestricted data sharing

(D) To ignore the impact of cyber threats

95. In the context of risk assessment, what does the term "vulnerability" refer to?

(A) A weakness that could be exploited by a threat

(B) Promoting unrestricted data sharing

(C) Ignoring potential risks

(D) Fostering a risk-aware culture

96. What is the purpose of a risk assessment report in cybersecurity risk management?

(A) To eliminate all vulnerabilities

(B) To promote unrestricted data sharing

(C) To communicate the results of the risk assessment

(D) To ignore potential risks

97. In the context of risk assessment, what does the term 'risk mitigation' involve?

(A) The process of identifying and assessing risks

(B) The process of eliminating all vulnerabilities

(C) The process of reducing the impact and likelihood of identified risks

(D) The process of promoting unrestricted data sharing

98. What is the purpose of a risk assessment policy in cybersecurity risk management?

(A) To eliminate all vulnerabilities

(B) To promote unrestricted data sharing

(C) To provide guidance on the risk assessment process and responsibilities

(D) To ignore potential risks

99. What is the purpose of a disaster recovery plan (DRP) in cybersecurity?

(A) To eliminate all vulnerabilities

(B) To promote unrestricted data sharing

(C) To ensure the restoration of IT services after a disruptive event

(D) To ignore potential risks

100. In the context of business continuity planning, what does the term "recovery point objective (RPO)" refer to?

(A) The maximum acceptable downtime for critical systems

(B) The point in time to which data must be recovered after a disruption

(C) The process of eliminating all vulnerabilities

(D) The impact of a risk on business operations

Rough Work / रफ कार्य

Example :

Question :

Q.1 Ⓐ ● Ⓒ Ⓓ

Q.2 Ⓐ Ⓑ ● Ⓓ

Q.3 Ⓐ ● Ⓒ Ⓓ

5. Each question carries equal marks. Marks will be awarded according to the number of correct answers you have.

6. All answers are to be given on OMR Answer Sheet only. Answers given anywhere other than the place specified in the answer sheet will not be considered valid.

7. Before writing anything on the OMR Answer Sheet, all the instructions given in it should be read carefully.

8. After the completion of the examination, candidates should leave the examination hall only after providing their OMR Answer Sheet to the invigilator. Candidate can carry their Question Booklet.

9. There will be no negative marking.

10. Rough work, if any, should be done on the blank pages provided for the purpose in the booklet.

11. To bring and use of log-book, calculator, pager & cellular phone in examination hall is prohibited.

12. In case of any difference found in English and Hindi version of the question, the English version of the question will be held authentic.

Impt. On opening the question booklet, first check that all the pages of the question booklet are printed properly. If there is any discrepancy in the question Booklet, then after showing it to the invigilator, get another question Booklet of the same series.

उदाहरण :

प्रश्न :

प्रश्न 1 Ⓐ ● Ⓒ Ⓓ

प्रश्न 2 Ⓐ Ⓑ ● Ⓓ

प्रश्न 3 Ⓐ ● Ⓒ Ⓓ

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।

6. सभी उत्तर केवल ओ०एम०आर० उत्तर-पत्रक (OMR Answer Sheet) पर ही दिये जाने हैं। उत्तर-पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।

7. ओ०एम०आर० उत्तर-पत्रक (OMR Answer Sheet) पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाये।

8. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी OMR Answer Sheet उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें। परीक्षार्थी अपने साथ प्रश्न-पुस्तिका ले जा सकते हैं।

9. निगेटिव मार्किंग नहीं है।

10. कोई भी रफ कार्य, प्रश्न-पुस्तिका में, रफ-कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।

11. परीक्षा-कक्ष में लॉग-बुक, कैल्कुलेटर, पेजर तथा सेल्युलर फोन ले जाना तथा उसका उपयोग करना वर्जित है।

12. प्रश्न के हिन्दी एवं अंग्रेजी रूपान्तरण में भिन्नता होने की दशा में प्रश्न का अंग्रेजी रूपान्तरण ही मान्य होगा।

महत्वपूर्ण: प्रश्नपुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्नपुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्नपुस्तिका प्राप्त कर लें।