Roll No.----------

प्रश्नपुस्तिका क्रमांक
Question Booklet No.
263680

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

BCA (Sixth Semester) Examination, 2024-25

(NEP)

(BCA6001)

INFORMATION & CYBER SECURITY

K-701

Paper Code							
A	6	0	0	0	1	1	T

(To be filled in the

प्रश्नपुस्तिका सीरीज
Question Booklet Series
D

SEA

Time : 1:30 Hours] [Maximum 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.

(Remaining instructions on the 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 हो या उसमें किसी अन्य प्रकार की कमी हो, तो उसे तुरन्त बदल लें।

(शेष निर्देश अन्तिम पृष्ठ पर)

1. Which of the following refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?

   (A) Cyber low

   (B) Cyberethics

   (C) Cybersecurity

   (D) Cybersafety

2. What is primary goal of ethical hacker :

   (A) Avoiding detection

   (B) Testing security vulnerability

   (C) Resolving security vulnerabilities

   (D) determining return on investment for security measures

3. In the computer networks, the encryption techniques are primarily used for improving the _____

   (A) Security

   (B) Performance

   (C) Reliability

   (D) Longevity

4. 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

5. Hash function are used for :

   (A) Encryption

   (B) Decryption

   (C) Digital signature

   (D) None of the above

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

(A) WPA

(B) WPA2

(C) WPS

(D) Both (A) and (C)

7. 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

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

(A) Over view

(B) Replaced

(C) Violated

(D) Changed

9. 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.

10. 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

11. Which of the following refers to the violation of the principle if a computer is no more accessible?

(A) Access control

(B) Confidentiality

(C) Availability

(D) All of the above

12. What is a firewall?

(A) Firewalls are network-based security measures that control the flow of incoming and outgoing traffic

(B) A firewall is a program that encrypts all the programs that access the Internet.

(C) A firewall is a program that keeps other programs from using the network.

(D) Firewalls are interrupts that automatically disconnect from the internet when a threat appears

13. Which of the following involves submitting as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests?

(A) Distributed denial-of-service attacks

(B) Backdoor

(C) Masquerading

(D) Phishing

14. Which of the following are possible security threats?

(A) Illegitimate use

(B) Backdoors

(C) Masquerading

(D) All of the given options are correct

15. Digital signatures provide which of the following ?

(A) Authentication

(B) Non-repudiation

(C) Integrity protection

(D) All of the given options are correct

16. Which of the following is valid difference between a Virus and a Spyware ?

(A) Spyware damages data and also steals sensitive private information

(B) Virus damages data, Spyware steals sensitive private information

(C) Spyware damages data, Virus steals sensitive private information

(D) Virus damages data and also steals sensitive private information

17. What is a computer virus?

(A) A virus is the same as a cookie in that it is stored on your computer against your permission.

(B) A virus is friendly software that is simply mislabeled.

(C) Malicious software that merely stays dormant on your computer.

(D) Malicious software that inserts itself into other programs.

18. Certification of Digital signature by an independent authority is needed because

(A) It is safe

(B) It gives confidence to a business

(C) The authority checks and assures customers that the public key indeed belongs to the business which claims its ownership

(D) Private key claimed by a sender may not be actually his

19. The responsibility of a certification authority for digital signature is to authenticate the :

(A) Hash function used

(B) Private keys of subscribers

(C) Public keys of subscribers

(D) key used in DES

20. Hashed message is signed by a sender using

(A) His public key

(B) His private key

(C) Receiver's public key

(D) Receiver's private key

21. A digital signature is

(A) A bit string giving identity of a correspondent

(B) A unique identification of a sender

(C) An authentication of an electronic record by tying it uniquely to a key only a sender knows

(D) an encrypted signature of a sender

22. All of the following are examples of real security and privacy threats except:

(A) Hackers

(B) Virus

(C) Spam

(D) Worm

23. What legal concept involves the unauthorized alteration or modification of data with the intent to deceive?

(A) Cyber terrorism

(B) Data breach

(C) Data manipulation

(D) Cyber extortion

24. What legal concept involves the unauthorized use of someone else's identity for fraudulent purposes?

(A) Cyber stalking

(B) Identity theft

(C) Spoofing

(D) Phishing

25. What legal concept involves using deception to trick individuals into revealing confidential information, such as passwords?

(A) Phishing

(B) Spoofing

(C) Cyber stalking

(D) Identity theft

26. Which of the following process is used for verifying the identity of a user?

(A) Authentication

(B) Identification

(C) Validation

(D) Verification

27. In the context of data protection, what does the term "data encryption" involve?

(A) Protecting personal data from unauthorized access by converting it into a non readable format

(B) Allowing unrestricted access to personal data

(C) Ignoring the security of personal data

(D) Promoting data processing without encryption

28. What legal principle allows individuals to control the collection and use of their personal information?

(A) Right to privacy

(B) Right to access

(C) Right to anonymity

(D) Right to be forgotten

29. What legal concept involves unauthorized access to computer systems with the intent to gather sensitive information?

(A) Cyber terrorism

(B) Cyber espionage

(C) Hacking

(D) Cyber stalking

30. What legal principle states that individuals have the right to know what information is collected about them and how it is used?

(A) Right to privacy

(B) Right to information

(C) Right to access

(D) Right to anonymity

31. What is the primary purpose of cyber laws and regulations?

(A) Restricting internet usage

(B) Protecting computer hardware

(C) Preventing cyber threats and crimes

(D) Promoting software development

32. Cyberspace has :

(A) No national boundaries

(B) International jurisdiction

(C) Limited boundaries

(D) (A) and (B)

33. 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

34. Which of the following statements is true about the Trojans?

(A) Trojans perform tasks for which they are designed or programmed

(B) Trojans replicates them self's or clone them self's through an infections

(C) Trojans do nothing harmful to the user's computer systems

(D) None of the above

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

(A) Rootkits

(B) Trojans

(C) Worms

(D) Viruses

36. Which of these systems use timestamps as an expiration date?

(A) Public-Key Certificates

(B) Public announcements

(C) Publicly available directories

(D) Public-Key authority

37. Which of the following public key distribution systems is most secure?

(A) Public-Key Certificates

(B) Public announcements

(C) Publicly available directories

(D) Public-Key authority

38. In the context of web security, what is an anomaly-based detection approach in IDS/IPS?

(A) Improving website aesthetics

(B) Blocking all incoming and outgoing traffic

(C) Identifying deviations from normal behavior patterns

(D) Granting unrestricted access to all users

39. How does an Intrusion Prevention System (IPS) differ from an IDS?

(A) By focusing on server performance

(B) By actively blocking malicious traffic in real-time

(C) By improving website aesthetics

(D) Granting unrestricted access to all users

40. What is the primary role of an Intrusion Detection System (IDS) in web security?

(A) Enhancing website aesthetics

(B) Actively blocking malicious traffic

(C) Monitoring and detecting potential security incidents

(D) Granting unrestricted access to all users

41. Cyber Security provide security against what?

(A) Against Malware

(B) Against cyber-terrorists

(C) Defends a device from threat

(D) All mentioned options

42. In order to ensure the security of the data/ information, we need to _____ the data:

(A) Encrypt

(B) Decrypt

(C) Delete

(D) None of the above

43. In the CIA Triad, which one of the following is not involved?

(A) Availability

(B) Confidentiality

(C) Authenticity

(D) Integrity

44. Which of the following is a type of independent malicious program that never required any host program?

(A) Trojan Horse

(B) Worm

(C) Trap Door

(D) Virus

45. Hackers usually used the computer virus for _____ purpose.

(A) To log, monitor each and every user's stroke

(B) To gain access the sensitive information like user's Id and Passwords

(C) To corrupt the user's data stored in the computer system

(D) All of the above

46. 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 & Malvertising

(C) Phishing and Password attacks

(D) All of the above

47. Which of the following can be considered as the elements of cyber security?

(A) Application Security

(B) Operational Security

(C) Network Security

(D) All of the above

48. _____ is a type of software designed to help the user's computer detect viruses and avoid them.

(A) Malware

(B) Adware

(C) Antivirus

(D) Both (B) and (C)

49. Which of the below does not constitute a cybercrime?

(A) Refusal of service

(B) Man in the middle

(C) Phishing

(D) MD5

50. Which of the below is a kind of cyber security?

(A) Cloud Security

(B) Application Security

(C) Cloud Security

(D) All options mentioned

51. How does a man-in-the-middle attack work?
(A) Overloading a server with traffic
(B) Intercepting and altering communication between two parties
(C) Spreading through infected email attachments
(D) Disguising itself as a legitimate program

52. An asymmetric-key (or public-key) cipher uses
(A) 1 key
(B) 2 key
(C) 3 key
(D) 4 key

53. Which of the following answers refers to a hierarchical system for the creation, management, storage, distribution, and revocation of digital certificates?
(A) SAAS
(B) DOS
(C) Digital signature
(D) Publik Key Infrastructure

54. The central node of 802.11 wireless operations is called.
(A) WPA
(B) Access Point
(C) WAP
(D) Access Port

55. The process of analyzing wireless traffic that may be helpful for forensic investigations or during troubleshooting any wireless issue is called?
(A) Wireless Traffic Sniffing
(B) Wireless Traffic Maltego
(C) Wireless Traffic BurpSuit
(D) Wireless Traffic Wireshark

56. Mobile security is also known as?
(A) OS Security
(B) APIs Security
(C) Wireless Security
(D) Database security

57. Which malware is designed to capture and transmit sensitive data, such as login credentials?

(A) Spyware

(B) Adware

(C) Keylogger

(D) Ransomware

58. What is true about data security?

(A) Data security is the protection of programs and data in computers and communication systems against unauthorized access

(B) It refers to the right of individuals or organizations to deny or restrict the collection and use of information

(C) Data security requires system managers to reduce unauthorized access to the systems by building physical arrangements and software checks.

(D) All of the above

59. Deleted files is a common technique used in computer forensics is the recovery of deleted files.

(A) TRUE

(B) FALSE

(C) Can be true or false

(D) Can not say

60. Computer forensics also be used in civil proceedings.

(A) Yes

(B) No

(C) Can be yes or no

(D) Can not say

61. 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

62. For ethical hacking, what process is followed

(A) Cryptography

(B) Encryption

(C) Decryption

(D) Penetration Testing

63. Digital signatures created and verified using

(A) Program

(B) graphical coding

(C) HTML

(D) cryptography

64. 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

65. 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

66. Which chapter of Cyber Law provides the legal Recognition to Digital Signature :

(A) Chapter III

(B) Chapter IV

(C) Chapter IX

(D) Chapter IX and X

67. Which type of malware is designed to observe and gather user information without their knowledge?

(A) Worm

(B) Trojan

(C) Spyware

(D) Adware

68. Password cracker tries

(A) Man in the middle attack

(B) Brute force attack

(C) Intrusion detection

(D) Intrusion prevention

69. e-governance include

(A) Filing of form online, paperless

(B) Efficient , low cost, transparent governance

(C) Both above

(D) Payment of bills

70. 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

71. What is the difference between vulnerability scanning and penetration testing?
(A) Vulnerability scanning identifies vulnerabilities and penetration testing exploits them
(B) B. Vulnerability scanning is an active process while penetration testing is passive
(C) Vulnerability scanning is less thorough than penetration testing
(D) Vulnerability scanning is conducted by internal security teams, while penetration testing is conducted by external security firms

72. PKI stands for?
(A) Public key infrastructure
(B) Private key infrastructure
(C) Public key instance
(D) Private key instance

73. Which of the following is a common type of vulnerability in web applications?
(A) Denial of service (DoS)
(B) SQL injection
(C) Man-in-the-middle (MitM) attack
(D) Buffer overflow

74. What is social engineering?
(A) Using force to gain access to the information you need
(B) Hacking either telecommunication or wireless networks to gain access to the information you need
(C) Using manipulation to deceive people that you are someone you are not to gain access to the information you need
(D) Using force to gain all the information available.

75. Which of the following is the best approach to conducting a penetration test?
(A) Black box testing
(B) White box testing
(C) Grey box testing
(D) Automated testing

76. Penetration testing should focus on what scenarios?

(A) Most likely.

(B) Most dangerous

(C) Both

(D) None

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

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

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

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

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

78. Is penetration testing used to help or for damaging a system?

(A) Helping

(B) Securing

(C) Damaging

(D) Both (A) & (C)

79. In public key cryptosystem for message confidentiality, which is kept as public?

(A) Decryption keys

(B) Encryption keys

(C) Encryption & Decryption keys

(D) None of the above

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

(A) Certified authority

(B) Subscriber

(C) Holder

(D) Controller

81. Which of the following is a general term for malicious software that pretends to be harmless so that a user willingly allows it to be downloaded onto the computer?

(A) Spware

(B) Virus

(C) Trojan Horse

(D) Botnets

82. 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

83. Which of the following type of attack can actively modify communications or data?

(A) Both Active and Passive attack

(B) Neither Active nor Passive attack

(C) Active attack

(D) Passive attack

84. Trojan Horse programs operate with what intent?

(A) To slowly but surely infect and become your operating system until the system crashes.

(B) To openly exploit a systems weaknesses until the user discovers it.

(C) To masquerade as non-malicious software while exploiting a system's weaknesses.

(D) To do a series of brute force attacks within the system itself and a series of external attacks from other servers

85. What is the purpose of a risk response strategy in the risk assessment process?

(A) To eliminate all vulnerabilities

(B) To promote unrestricted data sharing

(C) To outline the actions to be taken in response to identified risks

(D) To ignore potential risks

86. 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

87. 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

88. What is the purpose of a threat assessment in cybersecurity risk management?

(A) To eliminate all vulnerabilities

(B) To identify potential risks and threats

(C) To promote unrestricted data sharing

(D) To ignore the impact of threats

89. Which of the following is a key component of the risk assessment process?

(A) Ignoring potential risks

(B) Risk acceptance

(C) Promoting unrestricted access to sensitive data

(D) Fostering a risk-aware culture

90. 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

91. Which of the below is a popular victim of cyber attackers looking to gain the IP address of a target or victim user?

(A) emails

(B) websites

(C) IP tracer

(D) web pages

92. Which of the following is the collective name for Trojan horses, spyware, and worms?

(A) Spware

(B) Botnets

(C) Virus

(D) Malware

93. Which of the following is collection of Internet-connected programs communicating with other similar programs in order to perform tasks?

(A) Botnet

(B) Spyware

(C) Trojan horse

(D) Malware

94. Which of the following is a means to access a computer program or entire computer system bypassing all security mechanisms?

(A) Backdoor

(B) Masquerading

(C) Phishing

(D) Trojan Horse

95. There are two types of firewall. What are they?

(A) Internet-based and home-based.

(B) Hardware and software.

(C) Remote and local

(D) Digital and electronic.

96. A digital signature scheme consists of which of the following typical algorithms?

(A) Key generation, Signing and Signature verifying algorithm

(B) Signature verifying algorithm

(C) Key generation algorithm

(D) Signing algorithm

97. What is another name for an insecure plugin?

(A) Hardware

(B) Software

(C) Firmware

(D) Malware

98. 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

99. 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

100. 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

******

4. Four alternative answers are mentioned for each question as – A, B, C & D in the question booklet. The candidate has to choose the correct answer and mark the same in the OMR Answer-Sheet as per the direction :

Example :

Question :

Q. 1 (A) ● (C) (D)

Q. 2 (A) (B) ● (D)

Q. 3 (A) ● (C) (D)

Illegible answers with cutting and over-writing or half filled circle will be cancelled.

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 and 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.

4. प्रश्न–पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर– A; B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से एक सही उत्तर छाँटना है। उत्तर को OMR आन्सर–शीट में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

उदाहरण :

प्रश्न :

प्रश्न 1 (A) ● (C) (D)

प्रश्न 2 (A) (B) ● (D)

प्रश्न 3 (A) ● (C) (D)

अपठनीय उत्तर या ऐसे उत्तर जिन्हें काटा या बदला गया है, या गोले में आधा भरकर दिया गया, उत्तर निरस्त कर दिया जाएगा।

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।
6. सभी उत्तर केवल ओ. एम. आर. 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. ओ. एम. आर. 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 के अन्त में, रफ–कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।
11. परीक्षा–कक्ष में लॉग–बुक, कैलकुलेटर, 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 प्रश्न–पुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्न–पुस्तिका प्राप्त कर लें।