DO NOT OPEN THIS TEST BOOKLET UNTIL YOU ARE TOLD TO DO SO

Booklet Serial No. 000761

Test Booklet Series

A

TEST BOOKLET - 2022
SCIENTIFIC OFFICER CYBER FORENSIC
(08)

Time Allowed: Two Hours ***Maximum Marks: 120***

INSTRUCTIONS

1. IMMEDIATELY AFTER THE COMMENCEMENT OF THE EXAMINATION, YOU SHOULD CHECK THAT THIS TEST BOOKLET DOES ***NOT*** HAVE ANY UNPRINTED OR TORN OR MISSING PAGES OR ITEMS ETC. IF SO, GET IT REPLACED BY A COMPLETE TEST BOOKLET.

2. **Please note that it is the candidate's responsibility to encode and fill in the Roll Number and Test Booklet Series Code A, B, C or D carefully and without any omission or discrepancy at the appropriate places in the OMR Response Sheet. Any omission/discrepany will render the Response Sheet liable for rejection.**

3. You have to enter your Roll Number on the Test Booklet in the Box provided alongside. **DO NOT** write **anything else** on the Test Booklet.

4. This Test booklet contains **120** items (questions). Each item comprises of four responses (answers). You will select the response which you want to mark on the Response sheet. In case you feel that there is more than one correct response, mark the response which you consider the best. In any case, choose **ONLY ONE** response for each item.

5. You have to mark all your responses **ONLY** on the separate Response Sheet provided. See directions in the Response Sheet.

6. All items carry equal marks.

7. Before you proceed to mark in the Response sheet the response to various items in the Test Booklet you have to fill in some particulars in the Response Sheet as per instructions sent to you with your Admission Certificate.

8. After you have completed filling in all your responses on the Response Sheet and the examination has concluded, you should hand over to the Invigilator ***only the Response Sheet.*** You are permitted to take away with you the Test Booklet and Candidate's Copy of the Response Sheet.

9. Sheets for rough work are appended in the Test Booklet at the end.

10. **Penalty for wrong answers:**
    THERE WILL BE PENALTY FOR WRONG ANSWERS MARKED BY THE CANDIDATE.
    (i) There are four alternatives for the answer to every question. For each question for which a wrong answer has been given by the candidate, **0.25** of the marks assigned to that question will be deducted as penalty.
    (ii) It a candidate gives more than one answer, it will be treated as a **wrong answer** even if one of the given answers happens to be correct and there will be same penalty as above for that question.
    (iii) If a question is left blank, i.e., no answer is given by the candidate, there will be no **penalty** for that question.

SEAL

DO NOT OPEN THIS TEST BOOKLET UNTIL YOU ARE TOLD TO DO SO

1. Which of the following is an Electronic Evidence?

A) Hard Disk

B) RAM

C) Cloud Storage

D) All of these

2. CMOS Stands for ______________.

A) Computer Metal-Oxide Semiconductor

B) Complementary Metal-Oxide Semiconductor

C) Complementary Metal-Oxide Service

D) Complementary Metal-Oxide Semi- circuit

3. POST in computer stand for ______________.

A) Power On Self-Test

B) Power Off Self-Test

C) Power On Service-Test

D) Power Off Service-Test

4. Under which of the following sections of the Indian Information Technology Act 2000, an organization can be notified as an 'Examiner of Electronic Evidence'? [IT Act 2000]

A) 79z

B) 75a

C) 79a

D) 70a

5. VBR in storage media stands for ______________.

A) Volume Boot Record

B) Virtual Boot Record

C) Volume Base Record

D) Volume Boot Receiver

6. 1 Nibble = ______________ Bits

A) 01

B) 02

C) 03

D) 04

7. Data that has been deleted or partially overwritten are classified as ____________.

A) Active
B) Latent
C) Archival
D) Latest

8. NTFS stands from ____________.

A) New Tested File System
B) New Temporary File System
C) New Technology File System
D) No Technology File System

9. A ____________ sector is an area of the disk that can no longer be used to store data.

A) good
B) bad
C) free
D) test

10. File ____________ refers to the remaining unused bytes in the last sector of a file.

A) slack
B) size
C) length
D) width

11. The ____________ file is the area on a hard disk that stores an image of RAM.

A) Winsys
B) Cmd
C) Regedit
D) Page

12. Which of the following is not a type of FAT Filesystem?

A) FAT256
B) FAT16
C) FAT32
D) FAT12

13. A ____________ is a logical storage unit on a hard disk that contains contiguous sectors.

A) Byte
B) Nibble
C) Cluster
D) Sector

14. $(1011\ 1111)_2 = (\underline{\qquad})_{10}$

A) 190

B) 191

C) 192

D) 189

15. HPA stands for ____________.

A) Host Private Area

B) Home Protected Area

C) Host Public Area

D) Host Protected Area

16. DCO stands for ____________.

A) Device Control Overlays

B) Device Configuration Object

C) Device Configuration Overlays

D) Device Control Object

17. NTFS (version 1.0, also dubbed NT3 .1) first rolled out in August 1993 with __________.

A) Windows 98

B) Windows NT

C) Windows 95

D) Windows 93

18. $Bitmap is a file that contains one bit for each __________ in the partition.

A) Cluster

B) File

C) Picture

D) Directory

19. Which of the following is a cyber crime?

A) Website Defacement

B) Unauthorized Access

C) Creating Fake Profile on Social Media

D) All of the above

20. Which of the CIA component is compromised in DDoS attack?

A) Confidentiality

B) Integrity

C) Availability

D) None of the above

21. The __________ reference model was developed by the International Organization for Standardization in 1984 as an open standard for all communication systems to enable different types of networks to be linked together.

A) Open Software Interconnection (OSI)

B) Open Systems International (OSI)

C) Open Software International (OSI)

D) Open Systems Interconnection (OSI)

22. __________ layer of OSI reference model Handles end-to-end delivery to ensure error-free packets.

A) Network

B) Session

C) Transport

D) Data Link

23. a) A "reply from" response for the ping indicates that the connection to the server is up.

b) A "request timed out" response indicates that the network connection is up.

A) Both a) and b) are true

B) a) is true

C) b) is true

D) Both a) and b) are false

24. PPTP in VPN stand for __________.

A) Point to Point Tunneling Protocol

B) Point to Point Transport Protocol

C) Point to Point Transfer Protocol

D) Point to Point Transmission Protocol

25. The access method used in Wi-Fi networks is called __________.

A) CA/CA

B) CS/CA

C) CSMA/CA

D) CA/CSMS

26. __________ refers to the art and science of breaking ciphertext.

A) Cryptanalysis

B) Encryption

C) Decryption

D) Cryptography

27. If the formula for Encryption is E(M) = C then formula for Decryption can be written as __________.

A) D(M)=C

B) E(C) =M

C) D(C)=M

D) D(C) =E

28. __________ refers to a concept where the sender should not be able to falsely deny later that he sent a message.

A) Availability

B) Nonrepudiation

C) Integrity

D) Authentication

29. Asymmetric algorithms (also called __________ algorithms) are designed so that the key used for encryption is different from the key used for decryption.

A) Private-key

B) Personal-key

C) Public-key

D) Permanent -key

30. PKI stands for __________.

A) public key infrastructure

B) public key internet

C) private key infrastructure

D) private key internet

31. A computer __________ is just a collection of the instructions necessary to solve a specific problem.

A) Movie
B) Game
C) Program
D) RAM

32. After the program has been translated into an equivalent assembly language program, the next step in the compilation process is to translate the assembly language statements into actual __________.

A) machine syntax
B) instructions
C) code
D) machine instructions

33. In C Programming, the double type is very similar to the ____ type, but it is used whenever the range provided by a __________ variable is not sufficient.

A) Int
B) Char
C) Float
D) String

34. __________ is the malicious software that alters the regular functionality of an OS, takes full control on the targeted system and acts as the system administrator on the victim's system.

A) Rootkit
B) Trojan horse
C) Spyware
D) Malware

35. Explicit type conversions can be forced ("coerced") in any expression , with a unary operator called a __________.

A) Type
B) Data
C) Conversion
D) Cast

36. In OOP, using operators or functions in different ways , depending on what they are operating on, is called __________.

A) Polymorphism
B) Abstraction
C) Encapsulation
D) Inheritance

37. In C++, the identifier cout is actually a/an __________.

A) class

B) object

C) variable

D) alert

38. In C++, the operator << is called the __________ operator.

A) insertion or enter to

B) insertion or get from

C) insertion or put to

D) extraction or get from

39. A nibble is one digit of a hexadecimal (hex) value, which represents ____ bits.

A) 2

B) 3

C) 4

D) 5

40. 0x7DA2 = (__________ $)_{10}$.

A) 7,13,102

B) 32,162

C) 32,160

D) 7,12,102

41. In FAT, the directory entry is ______ bytes in length and contains the file's or directory's name, its size in bytes, its starting extent (or beginning cluster), and other file attributes or metadata.

A) 16

B) 128

C) 32

D) 64

42. You want to be able to track which users are accessing the C:\PAYROLL folder and whether the access requests are successful. Which of the following audit policy options allows you to track events related to file and print object access?

A) Audit Object Access

B) File and Object Access

C) Audit File and Print Access

D) Audit File and Object Access

43. On Windows devices, firewall logs can be found at %systemroot%\system32\LogFiles\Firewall\ ________.

A) firewall.log

B) msfirewall.log

C) mfirewall.log

D) pfirewall.log

44. The number of host bits in the IP address class A are ________.

A) 8

B) 16

C) 24

D) 32

45. In C Programming, the bitwise OR operator ¦ is used to turn bits ________.

A) Off

B) On

C) Negative

D) Positive

46. Which of the following is a syntactically correct representation of a FOR loop in C Programming?

A) for(i=0; i<10; i--)

B) for(i=0; i<1 0; i++)

C) for(;;)

D) All of these

47. In C programming, the unary operator ________ is the indirection or dereferencing operator; when applied to a pointer, it accesses the object the pointer points to.

A) &

B) *

C) !

D) ∧

48. In C Programming, the _______ operator only applies to objects in memory: variables and array elements. It cannot be applied to expressions, constants, or register variables.

A) &

B) *

C) !

D) ∧

49. In C Programming, if p is a pointer to a structure, then _______________ refers to the particular member.

A) p ← member-of-structure

B) p ↔ member-of-structure

C) p → member-of-structure

D) P * member-of-structure

50. _______ stops when it exhausts its format string, or when some input fails to match the control specification.

A) scanf

B) printf

C) getchar

D) putchar

51. In OOP, usually the data within a class is ________ and the functions are _______.

A) Public, Public

B) Public, Private

C) Private, Private

D) Private, Public

52. Some object-oriented languages refer to calls to member functions as _______.

A) Routines

B) Messages

C) Calls

D) None of these

53. A _______ is a member function that is executed automatically whenever an object is created.

A) GetData()

B) Destructor

C) Constructor

D) Function

54. A destructor has the same name as the constructor (which is the same as the class name) but is preceded by a __________ sign.

A) *

B) ~

C) !

D) &

55. Which function do we use for checking if a character is a space or a tab?

A) isdigit()

B) isblank()

C) isalnum()

D) isalpha()

56. A network address and the subnet mask 192.168.12.0 255.255.252.0 can be written in CIDR notation as _____________.

A) 192.168.12.0/255

B) 192.168.12.0/33

C) 192.168.12.0/22

D) 192.168.12.0/11

57. In subnet masking VLSM stands for __________.

A) Very-length subnet masking

B) Video-length subnet masking

C) Variable-large subnet masking

D) Variable-length subnet masking

58. An IPV6 address in which all 32 hexadecimal positions contain a value other than 0.

A) New IPv6 Address

B) Full IPv6 Address

C) Latest IPv6 Address

D) Final IPv6 Address

59. IEEE ______ was released in 2003 and was designed to enhance the technical capabilities of 802.11b and provide a speed of up to 54 Mbps.

A) 802.11g

B) 802.11c

C) 802.11i

D) 802.11z

60. The _______ is a pseudorandom identifier similar to a MAC address generated by the device creating the ad hoc network.

A) ICSSID

B) IDSSID

C) IBSSID

D) IISSID

61. If a file is small, sometimes its data is stored within the $MFT and is called _______ data.

A) sample

B) resident

C) foreign

D) global

62. In FAT32, location of File System Information, or the FSINFO is specified as a sector number at byte offsets _________ in the boot sector.

A) 20-25

B) 10-12

C) 0-2

D) 48-49

63. The BPB which stands for __________ is nothing more than a database of sorts, with defined fields that set forth the parameters of the partition and the file system within.

A) BIOS parameter block

B) Block parameter byte

C) BIOS parameter byte

D) Byte parameter block

64. The file signature (magic bytes) of a ZIP file is __________.

A) 50 3B 03 04

B) 50 4B 04 03

C) 50 4B 03 04

D) 50 4B 03 03

65. The __________ uses tracked changes to files for fast and efficient restoration of files when a system failure or power outage occurs.

A) Folder

B) Journal

C) Cluster

D) Block

66. A __________, also known as a data authentication code (DAC), is a one-way hash function with the addition of a secret key.

A) message access code

B) message automatic code

C) message authorization code

D) message authentication code

67. With respect to cryptography, the __________ protocol, invented by Ron Rivest and Adi Shamir has a good chance of foiling the man-in-the-middle attack.

A) Nomim

B) PreventMIM

C) Interlock

D) Locked

68. In Cryptography, __________ is a random string that is concatenated with passwords before being operated on by the one-way function

A) Salt

B) Key

C) Cipher

D) PKI

69. __________ are symmetric cryptography identification protocols developed for RACE'S RIPE project.

A) SKID and SKID2

B) SKID2 and SKID3

C) SKID2 and SKID4

D) SKID1, SKID2 and SKID3

70. Unlike normal digital signatures, an __________ signature cannot be verified without the signer's consent.

A) undeniable

B) abnormal

C) unknown

D) untouched

71. Demand paging relies on a characteristic of memory usage known as ____________, which is based on the observation that memory locations are likely to be frequently accessed in a short period time, as are their neighbors.

A) locality of memory

B) availability of reference

C) locality of reference

D) availability of memory

72. The application's data that needs to be dynamically allocated is stored within the region called the __________.

A) stack

B) heap

C) Slack

D) dma

73. A __________ is a range of memory that can be divided up into smaller blocks for storing any type of data that a kernel-mode component requests.

A) stack pool

B) stack space

C) kernel space

D) kernel pool

74. Windows tracks processes by assigning them a unique __________ structure that resides in a non-paged pool of kernel memory.

A) _PROCESS

B) _SPROCESS

C) _EPROCESS

D) _PROC

75. PEB in memory stands for __________.

A) Process Environment Block

B) Private Environment Block

C) Process Environment Byte

D) Private Environment Byte

76. As per the order of the volatility among the following which one is the most volatile?

A) Temporary File Systems

B) Routing Table

C) Memory

D) Swap Space

77. Which of the following is not a forensic image format?

A) dd

B) E01

C) raw

D) None of these

78. Which of the following registry hives is not a derived hive?

A) HKEY_USERS

B) HKEY_CURRENT_USER

C) HKEY_CLASSES_ROOT

D) HKEY_CURRENT_CONFIG

79. The superblock is a data structure found _______ bytes from the start of an Ext file system.

A) 256

B) 512

C) 1024

D) 2048

80. Note that Ext systems can be mounted with the _______ option, which will prevent all Accessed time stamp values on that volume from being updated.

A) noaccess

B) noatime

C) notime

D) noacesst

81. FAT12 supports maximum _________ clusters.

A) 4084

B) 1024

C) 2048

D) 65524

82. The boundary of each network can be found by applying a subnet mask to an IP address. This is simply a logical __________ operation IP address with the subnet mask.

A) OR

B) XOR

C) AND

D) NOT

83. One of the key differences between packet switching and circuit switching is that there is no fixed path between the __________, and each Packet may take a different route.

A) Protocols

B) LANs

C) Packets

D) Devices

84. CSMA/CA follows a simple process of RTS/CTS.

A) RTS/CTS

B) RTS/BTS

C) BTS/CTS

D) BTS/RTS

85. Which of the following operators cannot be overloaded in C++?

A) dot operator (.)

B) the scope resolution operator (::)

C) the conditional operator (?:)

D) All of these

86. In C Programming, the __________ statement is used to undefine something which was already defined.

A) #undef

B) #undo

C) #undefine

D) #defno

87. In C Programming, __________ function is used to test for an end-of-file condition on a file.

A) eof

B) end

C) feof

D) None of these

88. The __________ maintains a private list of the objects that you can use to cross- reference with other data sources.

A) client/server regular subsystem

B) client/server runtime subsystem

C) client/server runtime system

D) client/server runtime syntax

89. ASLR in memory stands for __________.

A) address space layout randomization

B) address system layout randomization

C) address space local randomization

D) address system local randomization

90. A process' __________ tree describes the layout of its memory segments at a slightly higher level than the page tables.

A) Binary

B) VAD

C) DAV

D) VAS

91. A __________ protocol is a routing algorithm that periodically sends the entire routing table to its neighboring or adjacent router.

A) distance vector
B) neighbor first
C) distance measure
D) neighborvectpr

92. EIGRP in network routing refers to __________.

A) Extended Interior Gateway Routing Protocol
B) Extensive Interior Gateway Routing Protocol
C) Exterior Interior Gateway Routing Protocol
D) Enhanced Interior Gateway Routing Protocol

93. Routers that support QoS can __________ network traffic.

A) forward
B) prioritize
C) read
D) question

94. For most IPv6 devices, __________ is the default option, and this became available in Windows 10.

A) SLACC
B) SLLAC
C) SLAAC
D) SLLAAC

95. __________ allows devices on separate IPv6 networks to communicate with each other across an IPv4 network.

A) 4to6
B) 6to4
C) I4toi6
D) i6toi4

96. If two graphs are identical except for the names of the points, they are called __________.

A) homorphic
B) polymorphic
C) isomorphic
D) biomorphic

97. There are two brute-force attacks against a one-way hash function: collision and __________.

A) Birthday
B) Daytime
C) Plain
D) None of these

98. Which of the following was a criterion for proposals for a standard cryptographic algorithm published by the NBS In the May 15, 1973.

A) The algorithm must provide a high level of security

B) The algorithm must be available to all users

C) The algorithm must be efficient to use

D) All of the above

99. __________ generators are pseudo-random-sequence generators.

A) Linear congestion

B) Linear congress

C) Linear congruential

D) Latest congruential

100. Padding in SHA is exactly the same as in __________.

A) AES

B) DES

C) MD4

D) MD5

101. *readelf* is distributed with __________ and is generally installed by default on all Linux distributions.

A) binutils

B) elfutils

C) elfbins

D) readutils

102. In Linux, one can find a number of static data structures with just the address in __________.

A) Address.map

B) Data.map

C) System.map

D) Structures.map

103. When drivers and kernel components write log messages, they store the messages within the kernel's debug ring buffer inside of __________ memory.

A) User

B) Kernel

C) Network

D) Secondary

104. The __________ keys are an important registry artifact used for determining what programs the user ran, as well as the time they were run.

A) Runmake

B) Allruns

C) Userassist

D) LastRuns

105. The Ex in the name VirtualAllocEx stands for __________.

A) External

B) Existing

C) Exceptional

D) Extra

106. PST which stands for __________ is the mail storage format used by Microsoft's Outlook email client.

A) Personal Storage Table

B) Personal Short Table

C) Public Storage Table

D) Public Short Table

107. Which of the following records resolve FQDNs to IPv6 addresses?

A) FFFF

B) AAAA

C) A

D) F

108. In MS Windows, Event Log records all contain a "magic number" or unique identifier which is __________.

A) EITI

B) EvTI

C) EvLv

D) LfLe

109. the $MFT file contains two sets of timestamps for files/directories: __________.

A) FNS and SIN

B) SIA and FNA

C) FIA and SNA

D) SAA and FII

110. In MS Windows, __________ contains a record of binaries that have executed on a system and also tracks executables that have been viewed through explorer.exe that have not been executed.

A) ShimCache

B) PECache

C) ExeCache

D) ShimExe

111. A/An __________ is an ad hoc network of up to eight Bluetooth devices, such as a computer, mouse, headset, earpiece, and so on.

A) octanet

B) piconet

C) bluenet

D) blueocta

112. WiMAX stands for __________.

A) Worldwide lnteroperability for Microwave Extension

B) Worldwide Interoperability for Microwave External

C) Worldwide Interoperability for Microwave Access

D) Worldwide Interoperability for Microwave Exceptional

113. The wildcard bits, also called the __________ bits, are used to match the network IP addresses (in A.B.C.D format) to interface IP addresses.

A) wild mask

B) inverse mask

C) reverse mask

D) exponential mask

114. SCSI Stands for __________.

A) Small Computer Systems Interface

B) Small Computer System small Interface

C) System Computer Systems Interface

D) Small Computer Small Interface

115. A process is an instance of a program executing in/on __________.

A) Network

B) Memory

C) Disk

D) Registry

116. Unlike fixed-size arrays and records, a __________ is intended to provide a flexible structure.

A) Variable

B) Constant

C) Linked-list

D) Header

117. __________ are often used in circumstances that require efficient insertions and searches where the data being stored is in <key, element> pairs.

A) 1-D Array

B) Variables

C) Base Tables

D) Hash Tables

118. The VAD tree is an example of a __________ binary tree that uses the memory address range as the key.

A) Self-creating

B) Self-deleting

C) Self-balancing

D) Self-editing

119. A __________ is a reference to an open instance of a kernel object, such as a file, registry key, mutex, process, or thread.

A) Thread

B) Handle

C) Stack

D) Heap

120. Shared libraries are generally stored on disk with the __________ extension.

A) .sl

B) .ls

C) .so

D) .s

ROUGH WORK

ROUGH WORK

SEAL