

15/06/22

पुस्तिका में पृष्ठों की संख्या-32

No. of Pages in Booklet -32

पुस्तिका में प्रश्नों की संख्या-150

No. of Questions in Booklet -150

Paper Code : 03

DAFC-22

3000017

प्रश्न पुस्तिका संख्या /
Question Booklet No.

SUBJECT : Cyber Forensic Division

समय : 2.30 घण्टे

Time: 2.30 Hours

अधिकतम अंक : 150

Maximum Marks: 150

प्रश्न पुस्तिका के पेपर सील/पॉलिथिन बैग को खोलने पर परीक्षार्थी यह सुनिश्चित कर लें कि प्रश्न पुस्तिका संख्या तथा ओ.एम.आर. उत्तर-पत्रक पर अंकित बारकोड समान हैं। इसमें कोई भिन्नता हो, तो परीक्षार्थी वीक्षक से दूसरा प्रश्न-पत्र प्राप्त कर लें। ऐसा सुनिश्चित करने की जिम्मेदारी अभ्यर्थी की होगी।

On opening the paper seal/polythene bag of the Question Booklet the candidate should ensure that Question Booklet Number and Barcode of OMR Answer Sheet must be same. If there is any difference, candidate must obtain another Question Booklet from Invigilator. Candidate himself shall be responsible for ensuring this.

परीक्षार्थियों के लिए निर्देश

1. सभी प्रश्नों के उत्तर दीजिए।
2. सभी प्रश्नों के अंक समान हैं।
3. प्रत्येक प्रश्न का केवल एक ही उत्तर दीजिए।
4. एक से अधिक उत्तर देने की दशा में प्रश्न के उत्तर को गलत माना जाएगा।
5. प्रत्येक प्रश्न के चार वैकल्पिक उत्तर दिये गये हैं, जिन्हें क्रमशः 1, 2, 3, 4 अंकित किया गया है। अभ्यर्थी को सही उत्तर निर्दिष्ट करते हुए उनमें से केवल एक गोले अथवा बबल को उत्तर-पत्रक पर नीले बॉल प्वाइंट पेन से गहरा करना है।
6. **OMR** उत्तर-पत्रक इस परीक्षा पुस्तिका के अन्दर रखा है। जब आपको परीक्षा पुस्तिका खोलने को कहा जाए, तो उत्तर-पत्रक निकाल कर ध्यान से केवल नीले बॉल प्वाइंट पेन से विवरण भरें।
7. प्रत्येक गलत उत्तर के लिए प्रश्न अंक का 1/3 भाग काटा जायेगा। गलत उत्तर से तात्पर्य अशुद्ध उत्तर अथवा किसी भी प्रश्न के एक से अधिक उत्तर से है। किसी भी प्रश्न से संबंधित गोले या बबल को खाली छोड़ना गलत उत्तर नहीं माना जायेगा।
8. मोबाइल फोन अथवा इलेक्ट्रॉनिक यंत्र का परीक्षा हॉल में प्रयोग पूर्णतया वर्जित है। यदि किसी अभ्यर्थी के पास ऐसी कोई वर्जित सामग्री मिलती है, तो उसके विरुद्ध आयोग द्वारा नियमानुसार कार्यवाही की जायेगी।
9. कृपया अपना रोल नम्बर ओ.एम.आर. पत्रक पर सावधानीपूर्वक सही भरें। गलत अथवा अपूर्ण रोल नम्बर भरने पर 5 अंक कुल प्राप्तांकों में से काटे जा सकते हैं।
10. यदि किसी प्रश्न में किसी प्रकार की कोई मुद्रण या तथ्यात्मक प्रकार की त्रुटि हो, तो प्रश्न के हिन्दी तथा अंग्रेजी रूपान्तरों में से अंग्रेजी रूपान्तर मान्य होगा।

चेतावनी : अगर कोई अभ्यर्थी नकल करते पकड़ा जाता है या उसके पास से कोई अनधिकृत सामग्री पाई जाती है, तो उस अभ्यर्थी के विरुद्ध पुलिस में प्राथमिकी दर्ज कराते हुए विविध नियमों-प्रावधानों के तहत कार्यवाही की जाएगी। साथ ही विभाग ऐसे अभ्यर्थी को भविष्य में होने वाली विभाग की समस्त परीक्षाओं से विवर्जित कर सकता है।

INSTRUCTIONS FOR CANDIDATES

1. Answer all questions.
2. All questions carry equal marks.
3. Only one answer is to be given for each question.
4. If more than one answers are marked, it would be treated as wrong answer.
5. Each question has four alternative responses marked serially as 1, 2, 3, 4. You have to darken only one circle or bubble indicating the correct answer on the Answer Sheet using **BLUE BALL POINT PEN**.
6. The **OMR Answer Sheet** is inside this Test Booklet. When you are directed to open the Test Booklet, take out the Answer Sheet and fill in the particulars carefully with blue ball point pen only.
7. **1/3 part of the mark(s) of each question will be deducted for each wrong answer.** A wrong answer means an incorrect answer or more than one answers for any question. Leaving all the relevant circles or bubbles of any question blank will not be considered as wrong answer.
8. Mobile Phone or any other electronic gadget in the examination hall is strictly prohibited. A candidate found with any of such objectionable material with him/her will be strictly dealt as per rules.
9. Please correctly fill your Roll Number in O.M.R. Sheet. **5 Marks** can be deducted for filling wrong or incomplete Roll Number.
10. If there is any sort of ambiguity/mistake either of printing or factual nature, then out of Hindi and English Version of the question, the English Version will be treated as standard.

Warning : If a candidate is found copying or if any unauthorized material is found in his/her possession, F.I.R. would be lodged against him/her in the Police Station and he/she would liable to be prosecuted. Department may also debar him/her permanently from all future examinations.

इस परीक्षा पुस्तिका को तब तक न खोलें जब तक कहा न जाए।

Do not open this Test Booklet until you are asked to do so.

1. A cache memory needs an access time of 30 ns and main memory 150 ns. What is the average access time of CPU? (Assume hit ratio = 80%)
 - (1) 60 ns
 - (2) 30 ns
 - (3) 150 ns
 - (4) 70 ns
2. An operating system with multiprogramming capability is one that allows -
 - (1) Several users to use the same program at once by giving each a slice of time.
 - (2) Loads several independent processes into memory and switches CPU from one job to another as required.
 - (3) Runs program over more than one processor
 - (4) None of the above
3. What does MIMD stands for?
 - (1) Multiple Instruction Memory Data
 - (2) Multiple Instruction Multiple Data
 - (3) Memory Instruction Multiple Data
 - (4) Memory Information Memory Data
4. Which of the following component does not belong to PCB (Process Control Block)?
 - (1) CPU Register
 - (2) CPU Scheduling Information
 - (3) Operating System Information
 - (4) Accounting Information
5. Which of the following binary formats supports the Linux Operating System?
 - (1) 0 and 1
 - (2) Binary Number format
 - (3) ELF Binary format
 - (4) None of these
1. यदि एक कैश मेमोरी को 30 ns और मुख्य मेमोरी को 150 ns के एक्सेस समय की आवश्यकता होती है, तो CPU का औसत एक्सेस समय क्या होगा? (hit ratio = 80% मान लें)
 - (1) 60 ns
 - (2) 30 ns
 - (3) 150 ns
 - (4) 70 ns
2. मल्टी प्रोग्रामिंग क्षमता वाला ऑपरेटिंग सिस्टम वह है, जो अनुमति देता है -
 - (1) कई उपयोगकर्ताओं को समय का एक टुकड़ा देकर एक ही प्रोग्राम को एक साथ उपयोग करने देना।
 - (2) कई स्वतंत्र प्रोसेसिज़ को मेमोरी में लोड करना और आवश्यकता अनुसार CPU को एक जॉब से दूसरे जॉब में स्विच करना।
 - (3) एक से अधिक प्रोसेसर पर प्रोग्राम चलाना।
 - (4) उपरोक्त में से कोई नहीं
3. MIMD से आप क्या समझते हैं?
 - (1) एकाधिक निर्देश मेमोरी डेटा
 - (2) एकाधिक निर्देश एकाधिक डेटा
 - (3) मेमोरी निर्देश एकाधिक डेटा
 - (4) मेमोरी निर्देश मेमोरी डेटा
4. निम्नलिखित में से कौनसा घटक PCB (Process Control Block) से संबंधित नहीं है?
 - (1) CPU रजिस्टर
 - (2) CPU शेड्यूलिंग की जानकारी
 - (3) Operating System की जानकारी
 - (4) लेखांकन की जानकारी
5. निम्न में से कौनसा बाइनरी प्रारूप Linux Operating System का समर्थन करता है?
 - (1) 0 और 1
 - (2) बाइनरी नंबर प्रारूप
 - (3) ELF बाइनरी प्रारूप
 - (4) इनमें से कोई नहीं

6. Consider a system with byte-addressable memory, 32 bit logical address, 4 kilobyte page size and page table entries of 4 bytes each. The size of the page table in system in megabytes is.....
- (1) 2 MB
 - (2) 4 MB
 - (3) 8 MB
 - (4) 16 MB
7. Which of the following register can interact with the Secondary Storage?
- (1) PC
 - (2) MAR
 - (3) MDR
 - (4) IR
8. In which allocation method does the user size the file before creating the file?
- (1) Contiguous
 - (2) Linked
 - (3) Indexed
 - (4) None of these
9. Which of the following is not a type of directory structure?
- (1) Acyclic-graph directory structure
 - (2) Single-level directory structure
 - (3) Tree structured directory
 - (4) Stack directory structure
10. If the page size increases, the internal fragmentation is.....
- (1) Decreases
 - (2) Increases
 - (3) Remains constant
 - (4) None of these
6. एक बाइट-एड्रेसेबल पर विचार करें जिसमें 32 bit का लॉजिकल एड्रेस हो, पेज की साइज़ 4 kB हो और प्रत्येक पेज टेबल एन्ट्री 4 bytes की हो, तो सिस्टम में पेज टेबल का आकार क्या होगा MB में?
- (1) 2 MB
 - (2) 4 MB
 - (3) 8 MB
 - (4) 16 MB
7. निम्न में से कौनसा रजिस्टर Secondary Storage के साथ interact कर सकता है?
- (1) PC
 - (2) MAR
 - (3) MDR
 - (4) IR
8. फाइल बनाने से पहले उपयोगकर्ता किस आवंटन विधि में फाइल को आकार देता है?
- (1) Contiguous
 - (2) Linked
 - (3) Indexed
 - (4) इनमें से कोई नहीं
9. निम्न में से कौन निर्देशिका संरचना का एक प्रकार नहीं है?
- (1) एक्रिलिक-ग्राफ निर्देशिका संरचना
 - (2) एकल-स्तरीय निर्देशिका संरचना
 - (3) ट्री संरचना निर्देशिका
 - (4) स्टैक संरचना निर्देशिका
10. यदि पृष्ठ का आकार बढ़ता है, तो आंतरिक विखंडन भी..... ।
- (1) कम हो जाता है
 - (2) बढ़ता है
 - (3) स्थिर रहता है
 - (4) इनमें से कोई नहीं

11. When a DNS server accepts and uses incorrect information from a host that have no authority of giving that information, then it is called.....
- (1) DNS Lookup
 - (2) DNS Hijacking
 - (3) DNS Spoofing
 - (4) None of the mentioned
12. If bandwidth in optical fiber communication is converted in terms of frequencies then those frequencies are in the range of -
- (1) Mega Hertz
 - (2) Gega Hertz
 - (3) Terra Hertz
 - (4) Kilo Hertz
13. The Protocol Data Unit (PDU) for the application layer in the Internet stack is -
- (1) Segment
 - (2) Datagram
 - (3) Message
 - (4) Frame
14. One of the Header fields in an IP datagram is the Time To Live (TTL) field. Which of the following statement best explains the need for this field?
- (1) It can be used to prioritize packets.
 - (2) It can be used to reduce delays.
 - (3) It can be used to optimize throughput.
 - (4) It can be used to prevent packet looping.
15. In the IPv4 addressing format, the number of networks allowed under class C addresses is -
- (1) 2^{14}
 - (2) 2^7
 - (3) 2^{21}
 - (4) 2^{24}
11. जब DNS सर्वर किसी होस्ट से गलत जानकारी स्वीकार करता है और उसका उपयोग करता है, जिसके पास उस जानकारी को देने का कोई अधिकार नहीं है, तो उसे कहा जाता है -
- (1) DNS लुकअप
 - (2) DNS अपहरण
 - (3) DNS स्पूफिंग
 - (4) उपरोक्त में से कोई नहीं
12. यदि ऑप्टिकल फाइबर संचार में बैंडविथ को आवृत्तियों के रूप में परिवर्तित किया जाता है, तो वे आवृत्तियाँ.....की सीमा में होती हैं।
- (1) Mega Hertz
 - (2) Gega Hertz
 - (3) Terra Hertz
 - (4) Kilo Hertz
13. इन्टरनेट स्टैक में application layer के लिए The Protocol Data Unit (PDU) है -
- (1) खंड
 - (2) डेटाग्राम
 - (3) संदेश
 - (4) फ्रेम
14. एक IP datagram में Header fields में से एक Time To Live (TTL) फील्ड है। निम्नलिखित में से कौनसा कथन इस क्षेत्र की आवश्यकता की सबसे अच्छी व्याख्या करता है?
- (1) इसका उपयोग पैकेट्स को प्राथमिकता देने के लिए किया जाता है।
 - (2) इसका उपयोग देरी को कम करने के लिए किया जा सकता है।
 - (3) इसका उपयोग थ्रूपुट को अनुकूलित करने के लिए किया जा सकता है।
 - (4) इसका उपयोग पैकेट लूपिंग को रोकने के लिए किया जा सकता है।
15. IPv4 addressing format में, class C एड्रेस के तहत अनुमत नेटवर्क की संख्या है -
- (1) 2^{14}
 - (2) 2^7
 - (3) 2^{21}
 - (4) 2^{24}

16. Suppose Computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use the same net mask N. Which of the values of N given below should not be used if A and B should belong to the same network?
- (1) 255.255.255.0
 - (2) 255.255.255.128
 - (3) 255.255.255.192
 - (4) 255.255.255.224
17. In a network of LANs connected by bridges, packets are sent from one LAN to another through intermediate bridges. Since more than one path may exist between two LAN's, packets may have to be routed through multiple bridges. Why is the spanning tree algorithm used for bridge-routing?
- (1) For shortest path routing between LAN's
 - (2) For avoiding Loops in the routing paths
 - (3) For fault tolerance
 - (4) for minimizing collisions
18. An organization has a class B network and wishes to form subnets for 64 departments. The subnet mask would be -
- (1) 255.255.0.0
 - (2) 255.255.64.0
 - (3) 255.255.128.0
 - (4) 255.255.252.0
16. मान लीजिए की Computers A और B के IP एड्रेस क्रमशः 10.105.1.113 और 10.105.1.91 हैं और वे दोनों एक ही नेटमास्क N का उपयोग करते हैं। नीचे दिए गए N के कौन से मान का उपयोग नहीं किया जाना चाहिए यदि A और B एक ही नेटवर्क से संबंधित हैं?
- (1) 255.255.255.0
 - (2) 255.255.255.128
 - (3) 255.255.255.192
 - (4) 255.255.255.224
17. पुलों से जुड़े LAN के नेटवर्क में पैकेट एक LAN से दूसरे LAN में मध्यवर्ती पुलों के माध्यम से भेजे जाते हैं। चूंकि दो LAN के बीच एक से अधिक पथ मौजूद हो सकते हैं, पैकेट को कई पुलों के माध्यम से राउट करना पड़ सकता है। पुल-राउटिंग के लिए स्पैनिंग tree algorithm का उपयोग क्यों किया जाता है?
- (1) LAN's के बीच सबसे छोटे राउटिंग पथ मार्ग के लिए
 - (2) राउटिंग पथ में लूप से बचने के लिए
 - (3) गलती सहनशीलता के लिए
 - (4) टकराव को कम करने के लिए
18. एक संगठन के पास class B नेटवर्क है और वह 64 विभागों के लिए सबनेट बनाना चाहता है, तो सबनेट मास्क होगा -
- (1) 255.255.0.0
 - (2) 255.255.64.0
 - (3) 255.255.128.0
 - (4) 255.255.252.0

19. Consider different activities related to e-mail :
- m1 : Send an e-mail from a mail client to a mail server.
- m2 : Download an e-mail from mailbox server to mail client.
- m3 : Checking e-mail in a web browser.
- Which is the application level protocol used in each activity?
- (1) m1 : HTTP m2 : SMTP m3 : POP
 (2) m1 : SMTP m2 : FTP m3 : HTTP
 (3) m1 : SMTP m2 : POP m3 : HTTP
 (4) m1 : POP m2 : SMTP m3 : IMAP
20. There is an arrangement where you allow an agency to host your website for you on their web server for a fee, this is called as-
- (1) Web Service
 (2) Web Hosting
 (3) Web Marketing
 (4) None of these
21. What type of password attack would be most successful against the password T63k#s23A?
- (1) Dictionary attack
 (2) Hybrid attack
 (3) Password guessing
 (4) Brute-force attack
22. Which of the following is a passive online attack?
- (1) Password guessing
 (2) Network sniffing
 (3) Brute-force attack
 (4) Dictionary attack
23. What type of hacking application is SNOW?
- (1) Password cracking
 (2) Privilege escalation
 (3) Spyware
 (4) Steganography
19. ई-मेल से संबंधित निम्न गतिविधियों पर विचार करें -
- m1 : Send an e-mail from a mail client to a mail server.
- m2 : Download an e-mail from mailbox server to mail client.
- m3 : Checking e-mail in a web browser.
- प्रत्येक गतिविधि में उपयोग किया जाने वाला Application स्तर protocol कौन सा है?
- (1) m1 : HTTP m2 : SMTP m3 : POP
 (2) m1 : SMTP m2 : FTP m3 : HTTP
 (3) m1 : SMTP m2 : POP m3 : HTTP
 (4) m1 : POP m2 : SMTP m3 : IMAP
20. एक ऐसी व्यवस्था जहाँ आप किसी एजेंसी को आपके वेब सर्वर पर शुल्क के लिए आपकी वेबसाइट होस्ट करने की अनुमति देते हैं, इसे कहा जाता है-
- (1) वेब सेवा
 (2) वेब होस्टिंग
 (3) वेब मार्केटिंग
 (4) इनमें से कोई नहीं
21. T63k#s23A पासवर्ड के खिलाफ किस प्रकार का पासवर्ड हमला सबसे सफल होगा?
- (1) शब्दकोष हमला
 (2) हाइब्रिड हमला
 (3) पासवर्ड अनुमान लगाना
 (4) पाशविक-बल हमला
22. निम्नलिखित में से कौन एक निष्क्रिय ऑनलाइन हमला है?
- (1) पासवर्ड अनुमान लगाना
 (2) नेटवर्क सूँघना
 (3) पाशविक-बल हमला
 (4) शब्दकोष हमला
23. SNOW किस प्रकार का हैकिंग application है?
- (1) पासवर्ड क्रैकर
 (2) विशेषाधिकार वृद्धि
 (3) स्पाइवेयर
 (4) स्टेगनोग्राफी

24. What is the most dangerous type of rootkit?
- (1) Kernel level
 - (2) Library level
 - (3) System level
 - (4) Application level
25. What is the difference between a Backdoor and a Trojan?
- (1) A Trojan usually provides a backdoor for a hacker.
 - (2) A backdoor must be installed first.
 - (3) A Trojan is not a way to access a system.
 - (4) A backdoor is provided only through a virus, not through a Trojan.
26. What is Ransomware?
- (1) Software that steals files from your computer and is used by blackmailers.
 - (2) A nickname for types of spyware that require a password on boot.
 - (3) A software that hijacks your computer and asks you to pay in order for it to be removed.
 - (4) Viruses that infect files and won't let you open them unless you know a certain passcode.
27. Which virus spreads through Word Macros?
- (1) Melissa
 - (2) Slammer
 - (3) Sobig
 - (4) Blaster
28. A virus that can cause multiple infections is known as what type of virus?
- (1) Multipartite
 - (2) Stealth
 - (3) Camouflage
 - (4) Multi-infection
24. रूटकिट का सबसे खतरनाक प्रकार क्या है?
- (1) कर्नेल स्तर
 - (2) लाइब्रेरी स्तर
 - (3) सिस्टम स्तर
 - (4) आवेदन स्तर
25. बैकडोर और ट्रोजन में क्या अन्तर है?
- (1) ट्रोजन आमतौर पर एक हैकर के लिए बैकडोर प्रदान करता है।
 - (2) पहले एक बैकडोर को स्थापित किया जाना चाहिए।
 - (3) ट्रोजन, सिस्टम को एक्सेस करने का तरीका नहीं है।
 - (4) बैकडोर केवल वायरस के माध्यम से प्रदान किया जाता है, ट्रोजन के माध्यम से नहीं।
26. रैंसमवेयर क्या है?
- (1) सॉफ्टवेयर जो कंप्यूटर से फाइलें चुराता है और ब्लैकमेलरों द्वारा उपयोग किया जाता है।
 - (2) स्पाइवेयर के प्रकार के लिए एक उपनाम जिसे बूट पर पासवर्ड की आवश्यकता होती है।
 - (3) एक सॉफ्टवेयर जो आपके कंप्यूटर को हाइजैक कर लेता है और इसे हटाने के लिए आपको भुगतान करने को कहता है।
 - (4) वायरस जो फाइलों को संक्रमित करते हैं और आपको उन्हें तब तक खोलने नहीं देते जब तक कि आप एक निश्चित पास कोड नहीं जानते हैं।
27. वर्ड मैक्रोस से कौनसा वायरस फैलता है?
- (1) मेलिसा
 - (2) स्लैमर
 - (3) सोबिग
 - (4) ब्लास्टर
28. एक वायरस जो कई संक्रमण पैदा कर सकता है उसे किस प्रकार के वायरस के रूप में जाना जाता है?
- (1) मल्टीपारटाईट
 - (2) स्टेल्थ
 - (3) कैमोफ्लेज
 - (4) मल्टी-इन्फैक्शन

29. Why would a Hacker use a proxy server?
- (1) To create a stronger connection with the Target.
 - (2) To create a ghost server on the network.
 - (3) To hide malicious activity on the network.
 - (4) To obtain a remote access connection.
30. DDoS in mobile systems wait for the owner of theto trigger the attack.
- (1) Botnets
 - (2) Programs
 - (3) Virus
 - (4) Worms
31. If an attacker manages to get an application to execute an SQL Query created by the attacker, then such attacks are called as –
- (1) SQL Attack
 - (2) SQL Injection Attack
 - (3) SQL Usage Attack
 - (4) SQL Destroyer Attack
32. What is necessary in order to install a hardware keylogger on target system?
- (1) The IP address of the system
 - (2) The administrator username and password
 - (3) Physical access to the system
 - (4) Telnet access to the system
33. An attack on a website that stores and displays text to a user is known as.....attack.
- (1) SQL Attack
 - (2) XSS Attack
 - (3) XRP Attack
 - (4) None of above mentioned
29. एक हैकर प्रॉक्सी सर्वर का उपयोग क्यों करता है?
- (1) लक्ष्य के साथ एक मजबूत संबंध बनाने के लिए।
 - (2) नेटवर्क पर एक घोस्ट सर्वर बनाने के लिए।
 - (3) नेटवर्क पर दुर्भावनापूर्ण गतिविधि छिपाने के लिए।
 - (4) रिमोट एक्सेस कनेक्शन प्राप्त करने के लिए।
30. मोबाइल सिस्टम में DDoS साइबर हमले को ट्रिगर करने के लिएके मालिक की प्रतीक्षा करता है?
- (1) बॉटनेट
 - (2) प्रोग्राम
 - (3) वायरस
 - (4) वर्म
31. यदि कोई हमलावर, हमलावर द्वारा बनाई गई SQL Query को निष्पादित करने के लिए एक application प्राप्त करने का प्रबंधन करता है, तो ऐसे हमलों को.....कहा जाता है।
- (1) SQL हमले
 - (2) SQL इंजेक्शन हमले
 - (3) SQL यूसेज हमले
 - (4) SQL विध्वंसक हमले
32. लक्ष्य प्रणाली पर hardware keylogger स्थापित करने के लिए क्या आवश्यक है?
- (1) सिस्टम का IP एड्रेस
 - (2) व्यवस्थापक का नाम और पासवर्ड
 - (3) प्रणाली तक भौतिक एक्सेस
 - (4) सिस्टम तक टैलनेट एक्सेस
33. एक वेबसाइट पर हमला जो उपयोगकर्ता के लिए text स्टोर और प्रदर्शित करता है, उसे..... हमले के रूप में जाना जाता है।
- (1) SQL हमला
 - (2) XSS हमला
 - (3) XRP हमला
 - (4) उल्लेखित में से कोई नहीं

34. The system where two independent pieces of data are used to identify a user is known as-
- (1) Two System Authentication
 - (2) ID Password Authentication
 - (3) Two Factor Authentication
 - (4) Multi data Authentication
35. Which of the following is not an example of offline password attacks?
- (1) Dictionary attacks
 - (2) Rainbow attacks
 - (3) Brute-force attacks
 - (4) Spamming attacks
36. Which of the following is a strong password?
- (1) 19thAugust88
 - (2) Delhi88
 - (3) P@assw0rd
 - (4) !augustdelhi
37. Which happens first, Authorization or Authentication?
- (1) Authorization
 - (2) Authentication
 - (3) Authorization and Authentication are same
 - (4) None of the mentioned
38. Which of the following is not a Strong Security Protocol?
- (1) HTTPS
 - (2) SSL
 - (3) SMTP
 - (4) SFTP
39. SSL primarily focuses on -
- (1) Integrity and Authenticity
 - (2) Integrity and non-repudiation
 - (3) Authenticity and privacy
 - (4) Confidentiality and integrity
40. Which of the following is a countermeasure for authentication hijacking?
- (1) Authentication logging
 - (2) Kerberos
 - (3) SSL
 - (4) Active Directory
34. वह प्रणाली जहाँ उपयोगकर्ता की पहचान करने के लिए डेटा के दो स्वतंत्र टुकड़ों का उपयोग किया जाता है -
- (1) दो सिस्टम प्रमाणीकरण
 - (2) आई.डी. पासवर्ड प्रमाणीकरण
 - (3) दो कारक प्रमाणीकरण
 - (4) मल्टी डेटा प्रमाणीकरण
35. इनमें से कौनसा ऑफलाइन पासवर्ड अटैक का उदाहरण नहीं है?
- (1) डिक्शनरी हमला
 - (2) रेनबो हमला
 - (3) पाशविक-बल हमला
 - (4) स्पैमिंग हमला
36. निम्न में से कौन एक स्ट्रॉन्ग पासवर्ड है?
- (1) 19thAugust88
 - (2) Delhi88
 - (3) P@assw0rd
 - (4) !augustdelhi
37. पहले कौनसा होता है, प्राधिकरण या प्रमाणीकरण?
- (1) प्राधिकरण
 - (2) प्रमाणीकरण
 - (3) प्राधिकरण और प्रमाणीकरण समान हैं
 - (4) उल्लिखित में से कोई नहीं
38. निम्नलिखित में से कौन एक मजबूत सुरक्षा प्रोटोकॉल नहीं है?
- (1) HTTPS
 - (2) SSL
 - (3) SMTP
 - (4) SFTP
39. SSL मुख्य रूप से.....पर केंद्रित है।
- (1) अखंडता और प्रमाणीकरण
 - (2) अखंडता और गैर-अस्वीकृति
 - (3) प्रमाणीकरण और गोपनीयता
 - (4) गोपनीयता और अखंडता
40. निम्नलिखित में से कौन प्रमाणीकरण हाइजैकिंग के लिए एक प्रत्युपाय है?
- (1) प्रमाणीकरण लॉगिंग
 - (2) Kerberos
 - (3) SSL
 - (4) सक्रिय निर्देशिका

41. Given the relations-
employee (name, salary, deptno) and
department (deptno, deptname, address)
Which of the following queries cannot be
expressed using the basic relational algebra
operation (U, -, x, π , σ , p)?

- (1) Department address of every employee
- (2) Employees whose name is same as their department name
- (3) The sum of all employees' salaries
- (4) All employees of a given department

42. Given the following relation instance –

X	Y	Z
1	4	2
1	5	3
1	6	3
3	2	2

Which of the following functional dependency are satisfied by instance?

- (1) $XY \rightarrow Z$ and $Z \rightarrow Y$
- (2) $YZ \rightarrow X$ and $Y \rightarrow Z$
- (3) $YZ \rightarrow X$ and $X \rightarrow Z$
- (4) $XZ \rightarrow Y$ and $Y \rightarrow X$

43. In SQL, relations can contain null values, and comparisons with null values are treated as unknown. Suppose all comparisons with a null value are treated as false. Which of the following pairs is not equivalent?

- (1) $x = 5$, not (not ($x = 5$))
- (2) $x = 5$, $x > 4$ and $x < 6$, where x is an integer
- (3) $x < 5$, not ($x = 5$)
- (4) None of the above

41. निम्न दिए गए संबंधों को देखते हुए—

कर्मचारी (नाम, वेतन, विभाग संख्या) और विभाग (विभाग संख्या, विभाग नाम, पता) निम्नलिखित में से कौन सी Query को मूल संबंधपटक बीजगणित का उपयोग करके (U, -, x, π , σ , p) संचालन व्यक्त नहीं किया जा सकता है?

- (1) प्रत्येक कर्मचारी के विभाग का पता
- (2) वे कर्मचारी जिनका नाम उनके विभाग के नाम के समान है
- (3) सभी कर्मचारियों के वेतन का योग
- (4) किसी दिए गए विभाग के सभी कर्मचारी

42. निम्नलिखित संबंध उदाहरण को देखते हुए –

X	Y	Z
1	4	2
1	5	3
1	6	3
3	2	2

निम्नलिखित में से कौन सी Functional Dependency उदाहरण से संतुष्ट होती है?

- (1) $XY \rightarrow Z$ और $Z \rightarrow Y$
- (2) $YZ \rightarrow X$ और $Y \rightarrow Z$
- (3) $YZ \rightarrow X$ और $X \rightarrow Z$
- (4) $XZ \rightarrow Y$ और $Y \rightarrow X$

43. SQL में संबंधों में null मान हो सकते हैं, और null मानों के साथ तुलना को अज्ञात के रूप में माना जाता है। मान लें कि एक null मान के साथ सभी तुलनाओं को गलत माना जाता है, तो निम्न में से कौन से जोड़े समतुल्य नहीं हैं?

- (1) $x = 5$, not (not ($x = 5$))
- (2) $x = 5$, $x > 4$ और $x < 6$, जहाँ x एक पूर्णांक है
- (3) $x < 5$, not ($x = 5$)
- (4) उपर्युक्त में से कोई नहीं

44. Consider a schema $R(A,B,C,D)$ and functional dependencies $A \rightarrow B$ and $C \rightarrow D$. Then the decomposition of R into $R_1(A, B)$ and $R_2(C, D)$ is -
- (1) Dependency preserving and lossless join
 - (2) Lossless but not dependency preserving
 - (3) Dependency preserving but not lossless join
 - (4) Not dependency preserving and not lossless join
45. Which of the following statements are TRUE about SQL Query?
- P: An SQL query can contain HAVING clause even if it does not have a GROUP BY clause.
- Q: An SQL query can contain a HAVING clause only if it has a GROUP BY clause.
- R: All attributes used in GROUP BY clause need to appear in SELECT clause.
- S: Not all attributes used in the GROUP BY clause need to appear in the SELECT clause:
- (1) P and R
 - (2) P and S
 - (3) Q and R
 - (4) Q and S
46. In the basic ER and relational models, which of the following statement is INCORRECT?
- (1) An attribute of an entity can have more than one value.
 - (2) An attribute of an entity can be composite.
 - (3) In a row of a relational table, an attribute can have more than one value.
 - (4) In a row of a relational table, an attribute can have exactly one value or a Null value.
44. Schema $R(A,B,C,D)$ और functional dependencies $A \rightarrow B$ और $C \rightarrow D$ पर विचार करें, तो R का $R_1(A, B)$ और $R_2(C, D)$ में अपघटन क्या है?
- (1) Dependency संरक्षण और lossless join
 - (2) Lossless join परन्तु Dependency संरक्षण नहीं
 - (3) Dependency संरक्षण परन्तु lossless join नहीं
 - (4) Dependency संरक्षण एवं lossless join दोनों ही नहीं
45. SQL query के बारे में निम्नलिखित में से कौन से कथन सत्य हैं?
- P: एक SQL Query में HAVING clause हो सकता है भले ही इसमें GROUP BY clause न हो।
- Q: एक SQL Query में HAVING clause तभी हो सकता है जब इसमें GROUP BY clause हो।
- R: GROUP BY clause में उपयुक्त होने वाले सभी Attributes, SELECT clause में आये, ऐसा जरूरी है।
- S: GROUP BY clause में उपयुक्त होने वाले सभी Attributes, SELECT clause में आये, ऐसा जरूरी नहीं है।
- (1) P और R
 - (2) P और S
 - (3) Q और R
 - (4) Q और S
46. मूल ER और संबंध परक मॉडल में निम्न में से कौन सा कथन गलत है?
- (1) एक Entity के Attribute में एक से अधिक मान हो सकते हैं।
 - (2) एक Entity का Attribute समग्र हो सकता है।
 - (3) एक relational table में एक row के attributes एक से अधिक मान के हो सकते हैं।
 - (4) एक relational table के एक row में एक attribute का केवल एक मान या Null मान हो सकता है।

47. Which of the following is TRUE?
- (1) Every relation in 2NF is also in BCNF.
 - (2) A relation R is in 3NF if every non-prime attribute of R is fully functionally dependent on every key of R.
 - (3) Every relation in BCNF is also in 3NF.
 - (4) No relation can be in both BCNF and 3NF.
48. Consider the following functional dependencies that hold for relations R (A,B,C) and S (B,D,E): $B \rightarrow A$, $A \rightarrow C$
The relation R contains 200 tuples and relation S contains 100 tuples. What is the maximum number of tuples possible in the natural join $R \bowtie S$ (R natural join S).
- (1) 100
 - (2) 200
 - (3) 300
 - (4) 2000
49. Which of the following are not a vulnerability – listed site/database?
- (1) Exploit - db
 - (2) Common Vulnerabilities and Exposures (CVE)
 - (3) National Vulnerability Database (NVD)
 - (4) Bing Vulnerability Database (BVD)
50. SQL authorization mechanism doesn't grants privileges on-
- (1) Specified attributes
 - (2) Specified tuples
 - (3) Entire relation
 - (4) None of the above
47. निम्नलिखित में से कौन सा कथन सत्य है?
- (1) 2NF का प्रत्येक relation, BCNF में भी होता है।
 - (2) एक Relation R 3NF में है यदि R की प्रत्येक गैर-अभाज्य attribute पूरी तरह से functionally dependent हो, R की प्रत्येक key पर।
 - (3) BCNF का प्रत्येक relation, 3NF में भी होता है।
 - (4) कोई भी relation BCNF और 3NF दोनों में नहीं हो सकता है।
48. Relations R (A,B,C) एवं S (B,D,E) : $B \rightarrow A$, $A \rightarrow C$ के लिए निम्नलिखित functional dependencies पर विचार करें।
यदि relation R में 200 tuples हैं और relation S में 100 tuples हैं, तो Natural Join $R \bowtie S$ (R Natural Join S) में संभव अधिकतम tuples की संख्या क्या होगी?
- (1) 100
 - (2) 200
 - (3) 300
 - (4) 2000
49. निम्न में से कौन सा एक vulnerability – listed साइट/डेटाबेस नहीं है?
- (1) एक्सप्लॉइट-डी.बी.
 - (2) कॉमन वल्नेरेबिलिटीज़ एण्ड एक्सपोज़र्स (CVE)
 - (3) राष्ट्रीय वल्नेरेबिलिटी डेटाबेस (NVD)
 - (4) बिंग वल्नेरेबिलिटी डेटाबेस (BVD)
50. SQL प्राधिकरण तंत्र विशेषाधिकार अनुदान नहीं देता है –
- (1) निर्दिष्ट attributes
 - (2) निर्दिष्ट tuples
 - (3) संपूर्ण relation
 - (4) उपर्युक्त में से कोई नहीं

51. In which of the following RC4 algorithm is not used?
- (1) SSL
 - (2) TLS
 - (3) WEP
 - (4) FTP
52. Which of the four operations are false for each round in the AES algorithm?
- (i) Substitute Bytes
 - (ii) Shift Columns
 - (iii) Mix Rows
 - (iv) XOR Round Key
- (1) (i) only
 - (2) (ii), (iii) and (iv)
 - (3) (ii) and (iv)
 - (4) Only (iv)
53. Using Rivest, Shamir, Adleman cryptosystem with $p = 7$ and $q = 9$, encrypt $M = 24$ to find ciphertext. The Ciphertext is -
- (1) 42
 - (2) 93
 - (3) 114
 - (4) 103
54. What is the number of round computation steps in the SHA-256 Algorithm?
- (1) 80
 - (2) 76
 - (3) 64
 - (4) 70
55. One of the Security Protocol for the e - mail system is -
- (1) IPSec
 - (2) SSL
 - (3) PGP
 - (4) None of the above
51. निम्नलिखित में से किस में RC4 एल्गोरिथम का उपयोग नहीं किया जाता है?
- (1) SSL
 - (2) TLS
 - (3) WEP
 - (4) FTP
52. AES algorithm में प्रत्येक दौर के लिए दिए गए 4 ऑपरेशनों में से कौन सा गलत है?
- (i) सबस्टिट्यूट Bytes
 - (ii) शिफ्ट Columns
 - (iii) मिक्स Rows
 - (iv) XOR राउंड Key
- (1) (i) केवल
 - (2) (ii), (iii) और (iv)
 - (3) (ii) और (iv)
 - (4) केवल (iv)
53. Rivest, Shamir, Adleman cryptosystem का उपयोग करके $p = 7$ और $q = 9$ के साथ और $M = 24$ को उपयोग करते हुए ciphertext खोजें। ciphertext है -
- (1) 42
 - (2) 93
 - (3) 114
 - (4) 103
54. SHA-256 Algorithm में गोल संगणना चरणों की संख्या क्या होती है?
- (1) 80
 - (2) 76
 - (3) 64
 - (4) 70
55. ई-मेल सिस्टम के लिए एक उचित सुरक्षा प्रोटोकॉल है।
- (1) IPSec
 - (2) SSL
 - (3) PGP
 - (4) उपरोक्त में से कोई नहीं

56. The combination of key exchange, hash, and encryption algorithm define a.....for each SSL session.
- (1) List of protocols
 - (2) Cipher suite
 - (3) List of keys
 - (4) None of the above
57. Which network security authentication method may be either software or hardware based to be used in a single login session or transaction?
- (1) Single Sign – On
 - (2) Two – factor authentication
 - (3) One – time password (OTP)
 - (4) Smart Card
58. Themethod provides a One-time session key for two parties.
- (1) Diffie-Hellman
 - (2) RSA
 - (3) DES
 - (4) AES
59. Which algorithm outputs a 128-bit message digest regardless of the length of the input?
- (1) SHA
 - (2) MD5
 - (3) RC4
 - (4) RC6
60. What is the purpose of a Hash?
- (1) To ensure confidentiality using public network such as internet.
 - (2) To ensure integrity of a transferred file.
 - (3) To ensure only authorized users are accessing file.
 - (4) To ensure that data is available to authorized users.
56. कुंजी विनिमय, हैश और Encryption Algorithm का संयोजन प्रत्येक SSL सत्र के लिए.....को परिभाषित करता है।
- (1) प्रोटोकॉलों की सूची
 - (2) सिफर सुइट
 - (3) कुंजीयों की सूची
 - (4) उपर्युक्त में से कोई नहीं
57. कौन सी नेटवर्क सुरक्षा प्रमाणीकरण विधि या तो Software या Hardware आधारित हो सकती है जिसका उपयोग एकल लॉगिन सत्र या लेनदेन में किया जा सकता है?
- (1) एकल साइन-ऑन (SSO)
 - (2) Two – factor प्रमाणीकरण
 - (3) One – Time पासवर्ड (OTP)
 - (4) Smart Card
58.विधि दो पार्टियों के लिए One – Time सत्र कुंजी प्रदान करती है।
- (1) डिफ़ी-हेलमैन
 - (2) RSA
 - (3) DES
 - (4) AES
59. कौन सी एल्गोरिथम इनपुट की लम्बाई की परवाह किए बिना 128-bit message digest आउटपुट प्रदान करती है?
- (1) SHA
 - (2) MD5
 - (3) RC4
 - (4) RC6
60. हैश का उद्देश्य क्या है?
- (1) इंटरनेट जैसे सार्वजनिक नेटवर्क का उपयोग करते समय गोपनीयता सुनिश्चित करने हेतु।
 - (2) किसी स्थानांतरित फाइल की अखंडता सुनिश्चित करने हेतु।
 - (3) यह सुनिश्चित करने के लिए कि केवल अधिकृत उपयोगकर्ता किसी फाइल को एक्सेस कर रहे हैं।
 - (4) यह सुनिश्चित करने के लिए के डेटा अधिकृत उपयोगकर्ताओं के लिए उपलब्ध है।

61. Which of the following tools best support the concept of breakpoints?
- (1) Debugger
 - (2) Sniffer
 - (3) Logger
 - (4) Disassembler
62. What are the 2 common phases of malware analysis?
- (1) Behavioural and code analysis
 - (2) Registry and file system analysis
 - (3) Identification and containment analysis
 - (4) User and kernel mode analysis
63. In the context of malware analysis, what does the term "patching" refer to?
- (1) Modifying a compiled executable to change its functionality without having to recompile it.
 - (2) Setting memory breakpoints by modifying access flags on memory segments.
 - (3) Stepping through the executable without running every instruction within function calls.
 - (4) Installing software updates that address vulnerabilities in installed software.
64. Which of the following system call is most likely to be used by a keylogger?
- (1) POP
 - (2) Virtual Alloc Ex
 - (3) Get Asyn key state
 - (4) Get Proc Address
65. Which malware enables administrative control, allowing an attacker to do almost anything on an infected computer?
- (1) Rootkits
 - (2) RATs
 - (3) Botnets
 - (4) Worms
61. निम्नलिखित में से कौन सा tool, breakpoints की अवधारणा का सबसे अच्छा समर्थन करता है?
- (1) डीबगर
 - (2) स्निफर
 - (3) लॉगर
 - (4) डिसअसेम्बलर
62. मैलवेयर विश्लेषण के दो सबसे आम चरण क्या हैं?
- (1) व्यवहार और कोड विश्लेषण
 - (2) रेजिस्ट्री और फाइल सिस्टम विश्लेषण
 - (3) पहचान और रोकथाम विश्लेषण
 - (4) उपयोगकर्ता और कर्नेल मोड विश्लेषण
63. मैलवेयर विश्लेषण के संदर्भ में, "पैचिंग" शब्द क्या संदर्भित करता है?
- (1) एक संकलित निष्पादन योग्य को संशोधित करना ताकि इसे recompile किए बिना इसकी कार्यक्षमता को परिवर्तित किया जा सके।
 - (2) स्मृति खंडों पर पहुँच ध्वज को संशोधित करके स्मृति विराम बिन्दु सेट करना।
 - (3) Function calls के भीतर हर निर्देश को चलाये बिना निष्पादन योग्य के माध्यम से कदम उठाना।
 - (4) सॉफ्टवेयर अद्यतनों को स्थापित करना जो स्थापित सॉफ्टवेयर में कमजोरियों को संबोधित करते हैं।
64. निम्नलिखित में से कौन से सिस्टम कॉल का एक keylogger द्वारा उपयोग किए जाने की सबसे अधिक संभावना है?
- (1) POP
 - (2) VirtualAllocEx
 - (3) GetAsynKeyState
 - (4) GetProcAddress
65. कौनसा मैलवेयर प्रशासनिक नियंत्रण को सक्षम करता है, जिससे एक हमलावर संक्रमित कम्प्यूटर पर लगभग कुछ भी करने की अनुमति देता है?
- (1) Rootkits
 - (2) RATs
 - (3) Botnets
 - (4) Worms

66. Which of the following malware do not replicate or reproduce through infection?
- (1) Worms
 - (2) Trojans
 - (3) Viruses
 - (4) Rootkits
67. What are the examples of Malware spreads?
- (1) Social network
 - (2) Pirated software
 - (3) Removable media
 - (4) All of the above
68. Which mechanism is malware least likely to use when defending itself against analysis?
- (1) Inserting junk code instructions
 - (2) Employing polarization techniques
 - (3) Making use of "tricky" jump instructions
 - (4) Detecting the presence of a debugger
69. Which of the following is possible sign of a malware infection?
- (1) Slow system performance
 - (2) Erratic computer behaviour
 - (3) Slow Internet connection
 - (4) All of the above
70. Rootkits are -
- (1) A set of software tools that enable an unauthorized user to gain control of a computer system without being detected.
 - (2) A network of private computers infected with malicious software and controlled as a group without the owner's knowledge.
 - (3) Kits used to treat online malware
 - (4) A type of greyware.
66. निम्नलिखित में से कौन सा मैलवेयर संक्रमण के माध्यम से दोहराता या पुनः उत्पन्न नहीं होता है?
- (1) Worms
 - (2) ट्रोजन
 - (3) वायरस
 - (4) Rootkits
67. मैलवेयर स्प्रेड के उदाहरण क्या हैं?
- (1) सामाजिक नेटवर्क
 - (2) पाइरेटेड सॉफ्टवेयर
 - (3) हटाने योग्य मीडिया
 - (4) उपरोक्त सभी
68. विश्लेषण के खिलाफ खुद का बचाव करते समय मैलवेयर द्वारा किस तंत्र के उपयोग की संभावना कम से कम है?
- (1) Junk code instructions सम्मिलित करना
 - (2) Polarization तकनीकों को नियोजित करना
 - (3) "मुश्किल" jump instructions का उपयोग करना
 - (4) डीबगर की उपस्थिति का पता लगाना
69. निम्नलिखित में से कौन सा मैलवेयर संक्रमण का संभावित संकेत है?
- (1) धीमी प्रणाली कार्यक्षमता
 - (2) अनियमित कम्प्यूटर व्यवहार
 - (3) Internet connection की धीमी गति
 - (4) उपरोक्त सभी
70. Rootkits हैं -
- (1) सॉफ्टवेयर उपकरणों का एक समूह जो किसी अनधिकृत प्रयोक्ता को, बिना पता लगाए, Computer system पर नियंत्रण प्राप्त करने में सक्षम बनाता है।
 - (2) Malicious Software से संक्रमित और मालिकों के ज्ञान के बिना एक समूह के रूप में नियंत्रित निजी computers का एक नेटवर्क।
 - (3) Online malware के इलाज के लिए उपयोग की जाने वाली किट।
 - (4) ग्रेवेयर का एक प्रकार।

71. A decision tree is pruned in order to -
- (1) Improve classification accuracy on training set
 - (2) Improve generalization performance
 - (3) Reduce dimensionality of the data
 - (4) Make the tree balanced
72. Which of the following criteria is not used to decide which attribute to split next in a decision tree?
- (1) Gini index
 - (2) Information gain
 - (3) Entropy
 - (4) Scatter
73. Which of the following is not a function of symbolic in the various function representation of machine learning?
- (1) Rules in proportional logic
 - (2) Hidden-Markov Models (HMM)
 - (3) Rules in first order predicate logic
 - (4) Decision Trees
74. What is the first step of FIND-S Algorithm?
- (1) Initialize 'h' to the most specific hypothesis in H.
 - (2) Generalize the 'h' by training example.
 - (3) Consider negative example for 'h'
 - (4) Both (1) and (2)
75. Which of the following is the limitation of FIND-S?
- (1) It has no way to determine the correct target concept.
 - (2) FIND-S will find the most specific hypothesis
 - (3) Handles consistent training examples
 - (4) All the above
71. एक decision tree काटा जाता है, ताकि -
- (1) प्रशिक्षण सेट पर वर्गीकरण सटीकता में सुधार हो सके
 - (2) सामान्यीकरण प्रदर्शन में सुधार हो सके
 - (3) डेटा की आयामिता को कम किया जा सके
 - (4) Tree को संतुलित किया जा सके
72. निम्नलिखित में से किस मानदंड का उपयोग यह तय करने के लिये नहीं किया जाता है, कि Decision Tree में आगे कौन सा attribute विभाजित करना है?
- (1) गिनी अनुक्रमणिका
 - (2) जानकारी प्राप्त करना
 - (3) एन्ट्रॉपी
 - (4) स्कैटर
73. निम्नलिखित में से कौन सा मशीन लर्निंग फंक्शन प्रतिनिधित्व में प्रतीकात्मक का कार्य नहीं है?
- (1) Proportional logic में नियम
 - (2) Hidden-Markov Models (HMM)
 - (3) प्रथम-क्रम विधेय तर्क में नियम
 - (4) Decision Trees
74. FIND-S Algorithm का पहला चरण क्या है?
- (1) H में सबसे विशिष्ट परिकल्पना के लिए 'h' प्रारंभ करना
 - (2) प्रशिक्षण उदाहरण द्वारा 'h' को सामान्यीकृत करना
 - (3) 'h' के लिए नकारात्मक उदाहरण पर विचार करना
 - (4) (1) और (2) दोनों
75. निम्नलिखित में से FIND-S की Limitation क्या है?
- (1) इसके पास सही लक्ष्य अवधारणा निर्धारित करने के लिए कोई तरीका नहीं है।
 - (2) FIND-S सबसे विशिष्ट अवधारणा परिकल्पना को खोजेगा
 - (3) लगातार प्रशिक्षण उदाहरण संभालना
 - (4) उपरोक्त सभी

76. What are the main components of big data?
- (1) HDFS
 - (2) MapReduce
 - (3) YARN
 - (4) All of the above
77. Transaction of data of the bank is a type is -
- (1) Unstructured
 - (2) Structured
 - (3) Both (1) and (2)
 - (4) None of the above
78. Identify among the options below, which is general-purpose computing model and runtime system for Distribution Data Analytics?
- (1) HDFS
 - (2) MapReduce
 - (3) Oozie
 - (4) All of the above
79. Which of the following is true about big data?
- (1) Big data can be processed using traditional techniques.
 - (2) Big data refers to Data Sets that are at least a petabyte in size.
 - (3) Big data analysis does not involve reporting and data mining techniques.
 - (4) Big data has low velocity meaning that it is generated slowly.
80. Which of the following are incorrect Big Data Technologies?
- (1) Apache Hadoop
 - (2) Apache Spark
 - (3) Apache Kafka
 - (4) Apache Pytarch
76. Big data के मुख्य घटक क्या हैं?
- (1) HDFS
 - (2) MapReduce
 - (3) YARN
 - (4) उपरोक्त सभी
77. बैंक के डेटा का लेन-देन किसका एक प्रकार है?
- (1) असंरचित
 - (2) संरचित
 - (3) (1) और (2) दोनों
 - (4) उपरोक्त में से कोई नहीं
78. नीचे दिये गये विकल्पों में से एक की पहचान करें जो Distributed Data Analytics के लिए सामान्य-उद्देश्य कम्प्यूटिंग मॉडल और रनटाइम सिस्टम है?
- (1) HDFS
 - (2) MapReduce
 - (3) Oozie
 - (4) उपरोक्त सभी
79. Big data के बारे में निम्नलिखित में से कौन सा कथन सत्य है?
- (1) Big data को पारंपरिक तकनीक का उपयोग करके संसाधित किया जा सकता है।
 - (2) Big data उन डेटा सेटों को संदर्भित करता है जो आकार में कम से कम एक petabyte होते हैं।
 - (3) Big data analysis में रिपोर्टिंग और डेटा mining तकनीक शामिल नहीं है।
 - (4) Big data में कम velocity होती है जिसका अर्थ धीरे-धीरे उत्पन्न होता है।
80. निम्न में से कौन सी Big Data Technologies सही नहीं है?
- (1) Apache Hadoop
 - (2) Apache Spark
 - (3) Apache Kafka
 - (4) Apache Pytarch

81. What makes WEP crackable?
- (1) Same key used for encryption and authentication
 - (2) Length of the key
 - (3) Weakness of IV
 - (4) RC4
82. A device that sends deauth frames is performing which type of attack against the WLAN?
- (1) Denial of Service
 - (2) Cracking
 - (3) Sniffing
 - (4) MAC spoofing
83. Which of the following is the best option for securing home wireless network?
- (1) WEP
 - (2) Shared-key authentication
 - (3) WPA-Personal
 - (4) WPA-Enterprise
84. What is the best way to enforce a "no wireless" policy?
- (1) Install a personal firewall
 - (2) Disable WLAN client adapters
 - (3) Use a WIDS/WIPS
 - (4) Only connect to open APs.
85. Which of the following is layer 7 application-secure protocols used to secure data on WLAN hotspots?
- (1) HTTPS
 - (2) HTTP
 - (3) FTP
 - (4) VPN
81. WEP को क्या क्रैक करने योग्य बनाता है?
- (1) Encryption और authentication के लिए एक ही key का काम में लेना
 - (2) Key की लंबाई
 - (3) IV की कमजोरी
 - (4) RC4
82. एक उपकरण जो deauth frames भेजता है, वह WLAN के खिलाफ किस प्रकार का हमला कर रहा है?
- (1) डिनायल ऑफ सर्विस
 - (2) क्रैकिंग
 - (3) स्निफिंग
 - (4) मैक स्पूफिंग
83. होम वायरलेस नेटवर्क को सुरक्षित करने के लिए निम्न में से कौन सा विकल्प सबसे अच्छा है?
- (1) WEP
 - (2) साझाकुंजी-प्रमाणीकरण
 - (3) WPA-व्यक्तिगत
 - (4) WPA-उद्यम
84. "नो वायरलेस" नीति करने का सबसे अच्छा तरीका क्या है?
- (1) एक व्यक्तिगत फायरवॉल स्थापित करें
 - (2) WLAN client adapters अक्षम करें
 - (3) WIDS/WIPS का प्रयोग करें
 - (4) केवल APs खोलने के लिए कनेक्ट करें
85. निम्नलिखित में से कौन से लेयर 7 application-secure protocol हैं जिसका उपयोग WLAN hotspot पर डेटा को सुरक्षित करने के लिए किया जाता है?
- (1) HTTPS
 - (2) HTTP
 - (3) FTP
 - (4) VPN

86. Which of the following is a countermeasure to using WEP?
- (1) Use a strong WEP key of at least 20 characters.
 - (2) Use a WEP key that does not repeat any of the same characters.
 - (3) Use WPA instead of WEP.
 - (4) Implement a preshared key with WEP.
87. Which is a common web server vulnerability?
- (1) Limited user accounts
 - (2) Default installation
 - (3) Open shares
 - (4) No directory access
88. Which of the following is the best countermeasure to session hijacking?
- (1) Port filtering firewall
 - (2) Encryption
 - (3) Session monitoring
 - (4) Strong passwords
89. What is called when a hacker inserts programmig commands into a web form?
- (1) Form tampering
 - (2) Command injection
 - (3) Biffer overflow
 - (4) Web form attack
86. निम्नलिखित में से कौन WEP का उपयोग करने के लिए एक प्रत्युपाय है?
- (1) कम से कम 20 वर्णों की सशक्त WEP key का उपयोग करें।
 - (2) एक ऐसी WEP key का उपयोग करें, जो समान वर्णों में से किसी को भी दोहराती नहीं है।
 - (3) WEP के बजाय WPA का प्रयोग करें।
 - (4) WEP के साथ एक साझा कुंजी लागू करें।
87. निम्न में से एक सामान्य वेब सर्वर भेद्यता कौन सी है?
- (1) सीमित उपयोगकर्ता खाते
 - (2) डिफॉल्ट स्थापना
 - (3) खुले शेयर
 - (4) कोई निर्देशिका एक्सेस नहीं
88. निम्नलिखित में से कौन प्रमाणीकरण हाइजैकिंग के लिए एक प्रतिवाद है?
- (1) पोर्ट फिल्टरिंग फायरवॉल
 - (2) एन्क्रिप्शन
 - (3) सेशन मॉनिटरिंग
 - (4) स्ट्रॉन्ग पासवर्ड
89. जब कोई हैकर वेब फॉर्म में programming कमांड डालता है, तो इसे क्या कहा जाता है?
- (1) फॉर्म से छेड़छाड़
 - (2) कमांड इंजेक्शन
 - (3) बफर ओवरफ्लो
 - (4) वेब फॉर्म अटैक

90. Which tool can be used to pull all e-mail addresses from a website?
- (1) Websleuth
 - (2) WSDigger
 - (3) Wget
 - (4) BlackWidow
91. Which among the following statement is not true about the Indian IT Act, 2000?
- (1) Came into force on 17th October, 2000.
 - (2) This act contains 84 sections.
 - (3) It gives legal validity to electronic contracts
 - (4) Both (1) and (2)
92. Which of the following network technologies uses a fibre – optic medium?
- (1) 802.11
 - (2) FDDI
 - (3) Ethernet
 - (4) Asynchronous transfer mode
93. CDRs in mobile forensics stands for -
- (1) Call Details Records
 - (2) Compact Disc Rewritable
 - (3) Compact Disc Readers
 - (4) Call Data Records
94. What does section 66E of IT Act, 2008 relate with?
- (1) Publishing private image of others
 - (2) Acts of cyber terrorism
 - (3) Cheating using computer resources
 - (4) Publishing child pornography
90. किसी वेबसाइट से सभी ई-मेल एड्रेसों को खींचने के लिए किस टूल का उपयोग किया जा सकता है?
- (1) Websleuth
 - (2) WSDigger
 - (3) Wget
 - (4) BlackWidow
91. भारतीय आई.टी. अधिनियम 2000 के बारे में कौन सा कथन सत्य नहीं है?
- (1) यह 17 अक्टूबर, 2000 को लागू हुआ।
 - (2) इस अधिनियम में 84 धाराएँ हैं।
 - (3) यह इलेक्ट्रॉनिक अनुबंधों को कानूनी वैधता देता है।
 - (4) (1) और (2) दोनों
92. निम्नलिखित में से कौन सी नेटवर्क तकनीक फाइबर ऑप्टिक माध्यम का उपयोग करती है?
- (1) 802.11
 - (2) FDDI
 - (3) इथरनेट
 - (4) अतुल्यकालिक स्थानांतरण मोड
93. मोबाइल फॉरेन्सिक में सी.डी.आर. का अर्थ है -
- (1) कॉल डिटेल्स रिकॉर्ड्स
 - (2) कॉम्पैक्ट डिस्क रिराइटेबल
 - (3) कॉम्पैक्ट डिस्क रीडर्स
 - (4) कॉल डेटा रिकॉर्ड्स
94. आई.टी. अधिनियम 2008 की धारा 66E किससे संबंधित है?
- (1) दूसरों की निजी छवि प्रकाशित करना
 - (2) साइबर आतंकवाद का कार्य
 - (3) कम्प्यूटर संसाधनों का उपयोग कर धोखाधड़ी
 - (4) चाइल्ड पोर्न प्रकाशित करना

95. JPEG is an acronym for -
- (1) Joint Photographic Extract Group
 - (2) Joint Photogenic Experts Group
 - (3) Joined Photographic Experts Graph
 - (4) Joint Photographic Experts Group
96. Select the incorrect statement about TDMA among the following options -
- (1) Discontinuous data transmission
 - (2) High transmission Rate
 - (3) Single carrier frequency for single user
 - (4) No requirement of duplexers
97. The process of documenting the seizure of digital evidence, and in particular, when that evidence changes hands is known as -
- (1) Field notes
 - (2) Interim report
 - (3) Chain of custody
 - (4) Digital report
98. Which statement is not true about 'Log Parser'?
- (1) It was initially written by Peter Adams.
 - (2) The default behaviour of log parser works like a 'data processing pipeline'.
 - (3) It is a powerful and versatile tool used as a web application forensic tool.
 - (4) It is a flexible command line utility.
99. The forensic copy of a device is a file called -
- (1) Volume image
 - (2) Video image
 - (3) Disc image
 - (4) Visual image
100. Which section of IT Act, 2008 deals with penalty for misrepresentation?
- (1) Section 70
 - (2) Section 71
 - (3) Section 71 (B)
 - (4) Section 73
95. JPEG का विस्तारित रूप है -
- (1) जॉइन्ट फोटोग्राफिक एक्सट्रेक्ट ग्रुप
 - (2) जॉइन्ट फोटोजेनिक एक्सपर्ट्स ग्रुप
 - (3) जॉइन्ड फोटोग्राफिक एक्सपर्ट्स ग्राफ
 - (4) जॉइन्ट फोटोग्राफिक एक्सपर्ट्स ग्रुप
96. निम्नलिखित में से टी.डी.एम.ए. के बारे में गलत कथन का चयन करें -
- (1) असंतत डेटा संचरण
 - (2) उच्च संचरण दर
 - (3) एकल उपयोगकर्ता के लिए एकल वाहक आवृत्ति
 - (4) डुप्लेक्सर्स की कोई आवश्यकता नहीं
97. डिजिटल साक्ष्य की जब्ती का दस्तावेजीकरण करने की प्रक्रिया और, विशेष रूप से, जब वह साक्ष्य हाथ बदलता है, को कहा जाता है -
- (1) फील्ड नोट्स
 - (2) अंतरिम रिपोर्ट
 - (3) चेन ऑफ कस्टडी
 - (4) डिजिटल रिपोर्ट
98. निम्न में से कौन सा कथन 'लॉग पार्सर' के बारे में सत्य नहीं है?
- (1) यह शुरू में पीटर एडम्स द्वारा लिखा गया था।
 - (2) लॉग पार्सर का डिफॉल्ट व्यवहार 'डेटा प्रोसेसिंग पाइपलाइन' की तरह काम करता है।
 - (3) यह शक्तिशाली और बहुमुखी उपकरण है, जिसका उपयोग वेब अनुप्रयोग फॉरेंसिक उपकरण के रूप में किया जाता है।
 - (4) यह एक लचीली कमांड लाइन उपयोगिता है।
99. एक डिवाइस की फॉरेंसिक कॉपी एक फाइल होती है, जिसे कहा जाता है -
- (1) वॉल्यूम इमेज
 - (2) वीडियो इमेज
 - (3) डिस्क इमेज
 - (4) विजुअल इमेज
100. आई.टी., अधिनियम 2008 की कौन सी धारा गलत बयानी के लिए दंड से संबंधित है?
- (1) धारा 70
 - (2) धारा 71
 - (3) धारा 71 (B)
 - (4) धारा 73

101. Which is not a tool or method for logical data extraction?
- (1) File system
 - (2) Android backups
 - (3) Advanced logical
 - (4) Chip-off method
102. The publication 'Guidelines on mobile device forensics' was published by -
- (1) ASTM
 - (2) IOCE
 - (3) NIST
 - (4) ENFSI
103. An attack where the attack source is more than one and often thousands of unique IP addresses-
- (1) DoS (Denial of Service) attack
 - (2) SQL Injection attack
 - (3) Website spoofing
 - (4) DDoS (Distributed Denial of Service) attack
104. What does CFIRP stands for -
- (1) Computed Forensic Incident Response Procedures
 - (2) Computer Forensic Incident Response Procedures
 - (3) Computer Forensic Incident Report Procedures
 - (4) Computer Forensic Incident Report Protocol
105. Which Section of IT Act defines Hacking with computer system?
- (1) Section 66 of IT Act
 - (2) Section 84 of IT Act
 - (3) Section 38 of IT Act
 - (4) Section 66E of IT Act
101. निम्न में से कौन सा तार्किक डेटा निष्कर्षण के लिए एक उपकरण या विधि नहीं है?
- (1) फाइल सिस्टम
 - (2) एंड्रॉइड बैकअप
 - (3) उन्नत तार्किक
 - (4) चिप-ऑफ विधि
102. 'गाइडलाइन्स ऑन मोबाइल फॉरेन्सिक्स' प्रकाशन किसके द्वारा प्रकाशित किया गया था?
- (1) ए.एस.टी.एम.
 - (2) आई.ओ.सी.ई.
 - (3) एन.आई.एस.टी.
 - (4) ई.एन.एफ.एस.आई.
103. एक हमला जहाँ हमले का स्रोत एक से अधिक होता है और अक्सर हजारों अद्वितीय आई.पी. एड्रेस होते हैं -
- (1) डिनाएल ऑफ सर्विस अटैक
 - (2) एस.क्यू.एल. इंजेक्सन हमला
 - (3) वेबसाइट स्पूफिंग
 - (4) डिस्ट्रीब्यूटेड डिनाएल ऑफ सर्विस अटैक
104. सी.एफ.आई.आर.पी. का अर्थ है -
- (1) कम्प्यूटेड फॉरेन्सिक इंसिडेन्ट रेसपॉन्स प्रोसीजर्स
 - (2) कम्प्यूटर फॉरेन्सिक इंसिडेन्ट रेसपॉन्स प्रोसीजर्स
 - (3) कम्प्यूटर फॉरेन्सिक इंसिडेन्ट रिपोर्ट प्रोसीजर्स
 - (4) कम्प्यूटर फॉरेन्सिक इंसिडेन्ट रिपोर्ट प्रोटोकॉल
105. कम्प्यूटर सिस्टम के साथ हैंकिंग आई.टी. का कौन सा सेक्शन परिभाषित करता है?
- (1) धारा 66, भारतीय आई. टी. अधिनियम,
 - (2) धारा 84, भारतीय आई. टी. अधिनियम,
 - (3) धारा 38, भारतीय आई. टी. अधिनियम,
 - (4) धारा 66E, भारतीय आई. टी. अधिनियम,

106. Which among the following was introduced in the amendments of Indian IT Act, 2008?
- (1) Penalties for voyeurism
 - (2) Penalties for pornography
 - (3) Penalties for child pornography
 - (4) Both (1) and (3)
107. What is the punishment for cyber terrorism?
- (1) Imprisonment for 10 years
 - (2) Life Imprisonment
 - (3) Imprisonment for 10 years along with fine of 5 lakh
 - (4) Imprisonment for 10 years along with fine of 10 lakh
108. Which cryptographic hash algorithm are a standard practice in digital forensics that is used in the preservation of digital evidence?
- (1) MD5 and SHA - 258
 - (2) MD5 and SHA - 1
 - (3) MD4 and SHA - 256
 - (4) MD4 and SHA - 2
109. Which of the following tool is not used for forensic analysis?
- (1) EnCase
 - (2) DEFT
 - (3) Log parser
 - (4) The Sleuth kit
110. Which among the following is NOT used in a WAP protocol suite?
- (1) Wireless Application Environment
 - (2) Wireless Session Protocol
 - (3) Wireless Transaction Protocol
 - (4) Wireless Transcription Protocol
111. What is the full form of GSM in mobile computing?
- (1) Global System for Mobile communication
 - (2) Global System for Moderate communication
 - (3) Graphic System for Mobile communication
 - (4) Global Service for Mobile communication
106. निम्नलिखित में से किसे भारतीय आई.टी. अधिनियम, 2008 के संशोधनों में पेश किया गया था?
- (1) दृश्यरतिकता के लिए दंड
 - (2) पोर्नोग्राफी के लिए दंड
 - (3) चाइल्ड पोर्नोग्राफी के लिए दंड
 - (4) (1) एवं (3) दोनों
107. साइबर आतंकवाद के लिए क्या सजा है?
- (1) 10 साल की कैद
 - (2) आजीवन कारावास
 - (3) 5 लाख जुर्माने के साथ 10 साल की कैद
 - (4) 10 लाख जुर्माने के साथ 10 साल की कैद
108. कौन सा क्रिप्टोग्राफिक हैश एल्गोरिथम डिजिटल फॉरेंसिक में एक मानक अभ्यास है जिसका उपयोग डिजिटल साक्ष्य के संरक्षण में किया जाता है?
- (1) एम.डी. 5 एवं एस.एच.ए.-258
 - (2) एम.डी. 5 एवं एस.एच.ए.-1
 - (3) एम.डी. 4 एवं एस.एच.ए.-256
 - (4) एम.डी. 4 एवं एस.एच.ए.-2
109. निम्न में से कौन सा उपकरण फॉरेंसिक विश्लेषण में उपयोग नहीं किया जाता है?
- (1) एनकेस
 - (2) डी.ई.एफ.टी.
 - (3) लॉगपार्सर
 - (4) दी स्लथ् किट
110. निम्न में से कौन सा WAP प्रोटोकॉल सूट में उपयोग नहीं किया जाता है?
- (1) वायरलेस अनुप्रयोग वातावरण
 - (2) वायरलेस सत्र प्रोटोकॉल
 - (3) वायरलेस लेनदेन प्रोटोकॉल
 - (4) वायरलेस ट्रांसक्रिप्शन प्रोटोकॉल
111. माबाईल कम्प्यूटिंग में जी.एस.एम. का विस्तारित नाम क्या है?
- (1) ग्लोबल सिस्टम फॉर मोबाईल कम्प्यूनिकेशन
 - (2) ग्लोबल सिस्टम फॉर मॉडरेट कम्प्यूनिकेशन
 - (3) ग्राफिक सिस्टम फॉर मोबाईल कम्प्यूनिकेशन
 - (4) ग्लोबल सर्विस फॉर मोबाईल कम्प्यूनिकेशन

112. Which code with specific character is used in transmission?
 (1) GSM
 (2) CDMA
 (3) RDMA
 (4) GPRS
113. Which of the following is not a asymmetric encryption decryption technique?
 (1) RSA
 (2) DST
 (3) XTR
 (4) DES
114. Which Section of IT Act, 2000 deals with publishing of information which is obscene in electronic form?
 (1) Section 66
 (2) Section 67
 (3) Section 68
 (4) Section 69
115. Which one of the following refers to the technique used for verifying the integrity of the message?
 (1) AES Algorithm
 (2) Decryption Algorithm
 (3) Digital Protocol
 (4) Message Digest
116. What is the punishment for stalking a women on the 1st offence in IPC?
 (1) Imprisonment of either description of term which may extend up to 3 years and shall be liable to fine.
 (2) Imprisonment of either description of term which may extend up to 5 years and liable to fine.
 (3) Imprisonment of either description of term which may extend up to 7 years.
 (4) Imprisonment of either description of term which may extend up to 5 years.
112. ट्रांसमिशन में विशिष्ट कैरेक्टर वाला कौन सा कोड प्रयोग किया जाता है?
 (1) जी.एस.एम.
 (2) सी.डी.एम.ए.
 (3) आर.डी.एम.ए.
 (4) जी.पी.आर.एस.
113. निम्नलिखित में से कौन असममित एन्क्रिप्शन डिक्रिप्शन तकनीक नहीं है?
 (1) आर.एस.ए.
 (2) डी.एस.टी.
 (3) एक्स.टी.आर.
 (4) डी.ई.एस.
114. आई.टी. अधिनियम, 2000 की कौन सी धारा इलेक्ट्रॉनिक रूप से अश्लील सूचना के प्रकाशन से संबंधित है?
 (1) धारा 66
 (2) धारा 67
 (3) धारा 68
 (4) धारा 69
115. निम्नलिखित में से कौन संदेश की सत्यता की पुष्टि करने के लिए प्रयोग की जाने वाली तकनीक को संदर्भित करता है ?
 (1) ए.ई.एस. एल्गोरिथम
 (2) डिक्रिप्शन एल्गोरिथम
 (3) डिजिटल प्रोटोकॉल
 (4) संदेश संग्रह
116. किसी महिला का पहली बार पीछा करने पर भारतीय दण्ड संहिता में सजा क्या है?
 (1) अवधि के किसी भी विवरण का कारावास जो की तीन साल तक बढ़ाया जा सकता है और जुर्माने के लिए उत्तरदायी।
 (2) अवधि के किसी भी विवरण का कारावास जो की पांच साल तक बढ़ाया जा सकता है और जुर्माने के लिए उत्तरदायी।
 (3) अवधि के किसी भी विवरण का कारावास जो की सात साल तक बढ़ाया जा सकता है।
 (4) अवधि के किसी भी विवरण का कारावास जो की पांच साल तक बढ़ाया जा सकता है।

117. Which of the following port and IP address scanner is famous among the users?
- (1) Cain and Abel
 - (2) Angry IP scanner
 - (3) Snort
 - (4) Ettercap
118. In Wi-Fi security, which of the following protocol is more used?
- (1) WPA
 - (2) WPA2
 - (3) WPS
 - (4) WPC2
119. In computer network, the encryption techniques are primarily used for improving the.....
- (1) Performance
 - (2) Security
 - (3) Reliability
 - (4) Longevity
120. In order to handle collision, Ethernet operates in 2 layers of the OSI model which are.....and.....
- (1) Physical layer and transport layer
 - (2) Application layer and data link layer
 - (3) Application layer and transport layer
 - (4) Physical layer and data link layer
121. Which of the following is not a type of scanning?
- (1) Xmas Tree Scan
 - (2) Cloud Scan
 - (3) Null Scan
 - (4) SYN Stealth
122. Which of the following is also referred to as 'malicious software'?
- (1) Maliciousware
 - (2) Badware
 - (3) Illegalware
 - (4) Malware
123. Which section of IPC deals with stalking?
- (1) Section 354 B
 - (2) Section 354 C
 - (3) Section 354 D
 - (4) Section 355
117. निम्नलिखित में से कौन सा पोर्ट एवं आई.पी. एड्रेस स्कैनर उपभोक्ताओं के बीच प्रसिद्ध है?
- (1) केन एवं ऐबल
 - (2) एंग्री आई.पी. स्कैनर
 - (3) स्नॉर्ट
 - (4) ईटरकैप
118. वाई-फाई सुरक्षा में, निम्न में से कौन सा प्रोटोकॉल ज्यादा उपयोग किया जाता है?
- (1) डब्ल्यू.पी.ए.
 - (2) डब्ल्यू.पी.ए.2
 - (3) डब्ल्यू.पी.एस.
 - (4) डब्ल्यू.पी.सी.2
119. कम्प्यूटर नेटवर्क में एन्क्रिप्शन तकनीकों का उपयोग मुख्य रूप से.....में सुधार के लिए किया जाता है।
- (1) प्रदर्शन
 - (2) सुरक्षा
 - (3) विश्वसनीयता
 - (4) लंबी उम्र
120. टक्कर को संभालने के लिए, ईथरनेट OSI मॉडल की 2 परतों में काम करता है, जो..... और..... हैं।
- (1) भौतिक परत और परिवहन परत
 - (2) आवेदन परत और डेटा लिंक परत
 - (3) आवेदन परत और परिवहन परत
 - (4) भौतिक परत और डेटा लिंक परत
121. निम्न में से कौन सा स्कैनिंग का प्रकार नहीं है?
- (1) एक्समस ट्री स्कैन
 - (2) क्लाउड स्कैन
 - (3) नल स्कैन
 - (4) एस.वाय.एन. स्टील्थ
122. निम्न में से किसे 'दुर्भावनापूर्ण सॉफ्टवेयर' भी कहा जाता है?
- (1) मैलेशियसवेयर
 - (2) बैडवेयर
 - (3) इलीगलवेयर
 - (4) मालवेयर
123. भारतीय दण्ड संहिता की कौन सी धारा स्टॉकिंग से संबंधित है?
- (1) धारा 354 B
 - (2) धारा 354 C
 - (3) धारा 354 D
 - (4) धारा 355

124. 'Digital Signature' is defined under which section of IT Act, 2000?
- (1) Section 2
 - (2) Section 11
 - (3) Section 6
 - (4) Section 8
125. In the year 2020, Indian Government banned 59 Chinese apps including TikTok, involving which section of IT Act, 2000 -
- (1) Section 66A
 - (2) Section 72A
 - (3) Section 69A
 - (4) Section 66F
126. What is it called when someone changes the 'FROM' section of an e-mail so that the message you receive appears to come from a person other than the one who sent it?
- (1) Spamming
 - (2) DoS
 - (3) Trooper
 - (4) Spoofing
127. Unsolicited commercial emails are commonly known as -
- (1) Hypertext
 - (2) Hoaxes
 - (3) Spam
 - (4) Phishing
128. Which of the following is not the commonly used programming language for artificial intelligence?
- (1) JAVA
 - (2) Perl
 - (3) PROLOG
 - (4) LISP
129. Face recognition system is based on which type of approach?
- (1) Weak AI approach
 - (2) Cognitive AI approach
 - (3) Applied AI approach
 - (4) Strong AI approach
124. 'डिजिटल हस्ताक्षर' को आई.टी. अधिनियम, 2000 की किस धारा के तहत परिभाषित किया गया है?
- (1) धारा 2
 - (2) धारा 11
 - (3) धारा 6
 - (4) धारा 8
125. वर्ष 2020 में भारत सरकार ने IT अधिनियम, 2000 की किस धारा को लागू करते हुए, TikTok सहित 59 चीनी ऐप्स पर प्रतिबंध लगा दिया था?
- (1) धारा 66 A
 - (2) धारा 72 A
 - (3) धारा 69 A
 - (4) धारा 66 F
126. इसे क्या कहते हैं, जब कोई व्यक्ति ई-मेल के 'फ्रॉम' सेक्शन को इस तरह बदल देता है कि आपको प्राप्त हुआ संदेश भेजने वाले के अलावा किसी अन्य व्यक्ति से आया है?
- (1) स्पैमिंग
 - (2) डी.ओ.एस.
 - (3) ट्रूपर
 - (4) स्पूफिंग
127. अवांछित वाणिज्यिक ईमेल को आमतौर पर कहा जाता है -
- (1) हाइपरटेक्स
 - (2) होक्स
 - (3) स्पैम
 - (4) फिशिंग
128. निम्नलिखित में से कौन कृत्रिम बुद्धि के लिये आमतौर पर इस्तेमाल की जाने वाली प्रोग्रामिंग भाषा नहीं है?
- (1) जावा
 - (2) पर्ल
 - (3) प्रोलोग
 - (4) लिस्प
129. फेस रिकग्निशन सिस्टम किस प्रकार के दृष्टिकोण पर आधारित है?
- (1) कमजोर ए.आई. दृष्टिकोण
 - (2) संज्ञानात्मक ए.आई. दृष्टिकोण
 - (3) एप्लाइड ए.आई. दृष्टिकोण
 - (4) मजबूत ए.आई. दृष्टिकोण

130.is a standard developed by the (ETSI) to describe the protocols for 2nd generation digital cellular networks used by mobile devices such as mobile phones and tablets.
- (1) Wireless Application Protocol (WAP)
 - (2) Advanced Mobile Phone System (AMPS)
 - (3) Global System for Mobile Communication (GSM)
 - (4) Global Navigation Satellite Systems (GNSS)
131. What is the size of IPv6 address?
- (1) 32 bits
 - (2) 64 bits
 - (3) 128 bits
 - (4) 256 bits
132. Which image compression provides some loss of quality?
- (1) Lossy
 - (2) Loss less
 - (3) Cell based
 - (4) Object based
133. What is the file extension name for the setup logs in Windows 7?
- (1) .log
 - (2) .stp
 - (3) .set
 - (4) .etl
134. Conversion of analog waves to digital format is called.....
- (1) Echo
 - (2) Frequency
 - (3) DAC
 - (4) Sampling
135. What was the original name of the Global Positioning System (GPS)?
- (1) P- GPS
 - (2) NAVSTAR – GPS
 - (3) Global GPS
 - (4) Original GPS
130. मोबाइल फोन और टैबलेट जैसे मोबाइल उपकरणों द्वारा उपयोग की जाने वाली दूसरी पीढ़ी के डिजिटल सेलुलर नेटवर्क के लिए प्रोटोकॉल का वर्णन करने के लिए (यूरोपीय दूर संचार मानक संस्थान) द्वारा विकसित एक मानक है—
- (1) वायरलेस एप्लिकेशन प्रोटोकॉल (WAP)
 - (2) उन्नत मोबाइल फोन प्रणाली (AMPS)
 - (3) मोबाइल संचार के लिए वैश्विक प्रणाली (GSM)
 - (4) ग्लोबल नेविगेशन सैटेलाइट सिस्टम्स (GNSS)
131. IPv6 एड्रेस का आकार क्या है?
- (1) 32 बिट्स
 - (2) 64 बिट्स
 - (3) 128 बिट्स
 - (4) 256 बिट्स
132. कौन सा छवि संपीड़न गुणवत्ता का कुछ नुकसान प्रदान करता है?
- (1) हानिपूर्ण
 - (2) नुकसान कम
 - (3) सेल आधारित
 - (4) वस्तु आधारित
133. विंडोज 7 में सेटअप लॉग के लिये फाइल एक्सटेंशन का नाम क्या है?
- (1) .log
 - (2) .stp
 - (3) .set
 - (4) .etl
134. एनालॉग तरंगों का डिजिटल प्रारूप में रूपांतरण क्या कहलाता है?
- (1) एको
 - (2) आवृत्ति
 - (3) डी.ऐ.सी.
 - (4) सैम्पलिंग
135. ग्लोबल पोज़िशनिंग सिस्टम (जीपीएस) का पुराना नाम क्या था?
- (1) पी – जीपीएस
 - (2) NAVSTAR—जीपीएस
 - (3) ग्लोबल जीपीएस
 - (4) ओरिजिनल जीपीएस

136. Which is the satellite navigation system that is operated by Russia as an alternative to GPS?
- (1) Global Navigation Satellite System (GLONASS)
 - (2) Russian Satellite System (RSS)
 - (3) Universal Navigation Satellite System (UNASS)
 - (4) There is no alternative satellite system
137. What type of interface does a DAQ (Data Acquisition) hardware creates?
- (1) Interface between 2 similar computers
 - (2) Interface between a computer and signal
 - (3) Interface between 2 dissimilar signals
 - (4) Interface between 2 similar signals
138. Video editing in Digital format is -
- (1) Non-linear editing
 - (2) Linear assemble editing
 - (3) In camera editing
 - (4) Sequential editing
139. In the US, the first commercial closed-circuit television system became available in 1949, is called -
- (1) Vericon
 - (2) Verizon
 - (3) I - zon
 - (4) I - con
140. Which tool is used to launch DDoS attack?
- (1) Jolt2
 - (2) TFN
 - (3) Targa
 - (4) Nemesis
141. Which of the following statement is NOT true about 'Melissa' worm?
- (1) It is also known as 'Kwejeebo'.
 - (2) It is also known as 'Kwyjibo'.
 - (3) It is also known as 'Kweyjibo'.
 - (4) It was written by David L. Smith.
136. जीपीएस के विकल्प के रूप में रूस द्वारा संचालित सैटेलाइट नेविगेशन सिस्टम कौन सा है?
- (1) ग्लोबल नेविगेशन सैटेलाइट सिस्टम (ग्लोनास)
 - (2) रशियन सैटेलाइट सिस्टम (RSS)
 - (3) यूनिवर्सल नेविगेशन सैटेलाइट सिस्टम (UNASS)
 - (4) कोई वैकल्पिक सैटेलाइट सिस्टम नहीं है
137. DAQ (डेटा अधिग्रहण) हार्डवेयर किस प्रकार का इंटरफेस बनाता है?
- (1) समान कम्प्यूटरों के बीच इंटरफेस
 - (2) कम्प्यूटर और सिग्नल के बीच इंटरफेस
 - (3) भिन्न सिग्नलों के बीच इंटरफेस
 - (4) समान सिग्नलों के बीच इंटरफेस
138. डिजिटल प्रारूप में वीडियो संपादन है -
- (1) गैर-रैखिक संपादन
 - (2) रैखिक इकट्ठा संपादन
 - (3) इन-कैमरा संपादन
 - (4) अनुक्रमिक संपादन
139. यूएस. में पहला वाणिज्यिक क्लोज्ड-सर्किट टेलीविजन सिस्टम 1949 में उपलब्ध हुआ, जिसे कहा जाता है?
- (1) वेरिकॉन
 - (2) वेरिजॉन
 - (3) आई-ज़ॉन
 - (4) आई-कॉन
140. DDoS अटैक लॉन्च करने के लिए किस टूल का उपयोग किया जाता है?
- (1) जॉल्ट2
 - (2) टीएफएन
 - (3) टार्गा
 - (4) नेमैसी
141. 'मेलिसा' वर्म के बारे में कौन सा कथन सत्य नहीं है?
- (1) इसे 'Kwejeebo' भी कहा जाता है।
 - (2) इसे 'Kwyjibo' भी कहा जाता है।
 - (3) इसे 'Kweyjibo' भी कहा जाता है।
 - (4) इसे डेविड एल. स्मिथ के द्वारा लिखा गया था।

142. XSS is -
- (1) Cross-Script Scripting
 - (2) Cross-Site Scripting
 - (3) Cross-Site Request Forgery
 - (4) Cross-Script Request Forgery
143. Which of the following cellular network does not follow standardized open protocol?
- (1) iDEN
 - (2) CDMA
 - (3) GSM
 - (4) TDMA
144. Which of the following type of noise is also known as 'photon noise'?
- (1) Reset noise
 - (2) Shot noise
 - (3) Hot pixel
 - (4) Dark noise
145. Match the following -
- | | |
|--------------------------|---|
| (a) Spherical aberration | (i) Light speckles in end image |
| (b) Coma | (ii) Less light reaches the periphery of the image plane compared to its center |
| (c) Light flame | (iii) Light does not converge into a sharp point |
| (d) Vignetting | (iv) Inconsistent refraction of light at the lens center |
- (1) (a)-(iii), (b)-(iv), (c)-(i), (d)-(ii)
 - (2) (a)-(ii), (b)-(iv), (c)-(iii), (d)-(i)
 - (3) (a)-(iii), (b)-(i), (c)-(iv), (d)-(ii)
 - (4) (a)-(ii), (b)-(iv), (c)-(i), (d)-(iii)
142. एक्स.एस.एस. है-
- (1) क्रॉस-स्क्रिप्ट स्क्रिप्टिंग
 - (2) क्रॉस-साइट स्क्रिप्टिंग
 - (3) क्रॉस-साइट रिक्वेस्ट फॉर्जरी
 - (4) क्रॉस-स्क्रिप्ट रिक्वेस्ट फॉर्जरी
143. निम्नलिखित में से कौन सा सेलुलर नेटवर्क मानकीकृत खुले प्रोटोकॉल का पालन नहीं करता है?
- (1) आई.डी.ई.एन.
 - (2) सी.डी.एम.ए.
 - (3) जी.एस.एम.
 - (4) टी.डी.एम.ए.
144. निम्न में से किस प्रकार के शोर को 'फोटॉन नॉइज़' के रूप में भी जाना जाता है?
- (1) रीसेट नॉइज़
 - (2) शॉट नॉइज़
 - (3) हॉट पिक्सेल
 - (4) डार्क नॉइज़
145. निम्नलिखित को मिलाएं -
- | | |
|-------------------|---|
| (a) गोलाकार विपथन | (i) अंत छवि में हल्के धब्बे |
| (b) कोमा | (ii) इसके केंद्र की तुलना में कम प्रकाश छवि तल की परिधि तक पहुंचता है |
| (c) फ्लेम लाइट | (iii) प्रकाश एक नुकीले बिन्दु में परिवर्तित नहीं होता है |
| (d) विगनेटिंग | (iv) लेंस केंद्र पर प्रकाश का असंगत अपवर्तन |
- (1) (a)-(iii), (b)-(iv), (c)-(i), (d)-(ii)
 - (2) (a)-(ii), (b)-(iv), (c)-(iii), (d)-(i)
 - (3) (a)-(iii), (b)-(i), (c)-(iv), (d)-(ii)
 - (4) (a)-(ii), (b)-(iv), (c)-(i), (d)-(iii)

146. In DCT (Discrete Cosine transform), pixel values are shifted from unsigned integers in the range $[0, 2^b - 1]$ to signed integers in the range -
- (1) $[-2^{b-1}, -2^{b-1}-1]$
 - (2) $[2^{b-1}, -2^{b-1}-1]$
 - (3) $[-2^{b-1}, 2^b - 1]$
 - (4) $[2^{b-1}, 2^{b-1}-2]$
147. The tool 'ElSave' was written by -
- (1) Jesper Lauritsen
 - (2) David L. Smith
 - (3) Gabriele Giuseppini
 - (4) Peter Adams
148. 'IMEI' stands for -
- (1) International Modern Equipment Identity
 - (2) Internal Mobile Equipment Identity
 - (3) International Mobile Equipment Identity
 - (4) Internal Modern Equipment Identity
149.is a standard system for Analog signal cellular telephone service in the United States.
- (1) TDMA
 - (2) GSM
 - (3) AMPS
 - (4) NTT DOCOMO
150. Mobile telephone was invented and patented by -
- (1) Nathan B. Stubblefield
 - (2) Nate B. Stubblefield
 - (3) Nathan B. Stanfield
 - (4) Nate B. Stanfield
146. DCT (असतत कोसाइन ट्रांसफॉर्म) में, पिक्सेल मानों को स्थानांतरित किया जाता है, श्रेणी $[0, 2^b - 1]$ के अहस्ताक्षरित पूर्णाकों से, श्रेणी के हस्ताक्षरित पूर्णाकों तक।
- (1) $[-2^{b-1}, -2^{b-1}-1]$
 - (2) $[2^{b-1}, -2^{b-1}-1]$
 - (3) $[-2^{b-1}, 2^b - 1]$
 - (4) $[2^{b-1}, 2^{b-1}-2]$
147. उपकरण 'एल्सेव' किसके द्वारा लिखा गया था?
- (1) जेस्पर लॉरिट्सन
 - (2) डेविड एल. स्मिथ
 - (3) गेब्रियल ग्यूसेपिनी
 - (4) पीटर एडम्स
148. आई.एम.ई.आई. का अर्थ है -
- (1) इंटरनेशनल मॉडर्न इक्युपमेंट आइडेनटिटी
 - (2) इंटरनल मोबाइल इक्युपमेंट आइडेनटिटी
 - (3) इंटरनेशनल मोबाइल इक्युपमेंट आइडेनटिटी
 - (4) इंटरनल मॉडर्न इक्युपमेंट आइडेनटिटी
149.संयुक्त राज्य अमेरिका में एनालॉग सिग्नल सेलुलर टेलीफोन सेवा के लिए एक मानक प्रणाली है।
- (1) टी.डी.एम.ए.
 - (2) जी.एस.एम.
 - (3) ए.एम.पी.एस.
 - (4) एन.टी.टी. डोकोमो
150. मोबाइल टेलीफोन का अविष्कार और पेटेंट किसके द्वारा किया गया था?
- (1) नाथन बी. स्टबलफील्ड
 - (2) नैट बी. स्टबलफील्ड
 - (3) नाथन बी. स्टैनफील्ड
 - (4) नैट बी. स्टैनफील्ड

Space for Rough Work / रफ कार्य के लिए जगह