

पुस्तिका में पृष्ठों की संख्या-24

No. of Pages in Booklet -24

पुस्तिका में प्रश्नों की संख्या-150

No. of Questions in Booklet -150

Paper Code : 05

**SUBJECT : Cyber Forensic Division**

15/06/22

**OSSFC-22**

5000081

प्रश्न पुस्तिका संख्या /  
Question Booklet No.

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. The access time of a sequentially accessed memory is-
  - (1) Same as that of a RAM
  - (2) Less than that of a RAM
  - (3) Higher than that of a RAM
  - (4) Same as that of a ROM
2. Which was the first computer based on stored program concept?
  - (1) ENIAC
  - (2) EDVAC
  - (3) UNIVACI
  - (4) IBM - 701
3. Which register holds the address of the active memory location?
  - (1) Instruction register
  - (2) Program control register
  - (3) Accumulator register
  - (4) Memory address register
4. Which one is an open - source operating system?
  - (1) Unix
  - (2) Windows
  - (3) Linux
  - (4) MS - DOS
5. Virtual memory is-
  - (1) An extremely large main memory
  - (2) An extremely large secondary memory
  - (3) An illusion of an extremely large memory
  - (4) A type of memory used in super computers
6. The processing speed of CPU is closer to which memory?
  - (1) Cache Memory
  - (2) Random Access Memory
  - (3) Read Only Memory
  - (4) Virtual Memory
7. Mapping of file is managed by-
  - (1) Virtual Memory
  - (2) File metadata
  - (3) File system
  - (4) None of the above
1. अनुक्रमिक अभिगम मेमोरी का access time होता है -
  - (1) रैम के बराबर
  - (2) रैम से कम
  - (3) रैम की तुलना में ज्यादा
  - (4) रोम के बराबर
2. स्टोर्ड प्रोग्राम आधारित प्रथम कम्प्यूटर कौन सा है?
  - (1) ENIAC
  - (2) EDVAC
  - (3) UNIVACI
  - (4) IBM - 701
3. ऐक्टिव मेमोरी लोकेशन किस रजिस्टर के द्वारा hold (संग्रहित) किया जाता है?
  - (1) इंस्ट्रक्शन रजिस्टर
  - (2) प्रोग्राम कंट्रोल रजिस्टर
  - (3) एक्यूमलेटर रजिस्टर
  - (4) मेमोरी एड्रेस रजिस्टर
4. निम्न में से ओपन सोर्स ऑपरेटिंग सिस्टम कौन सा है?
  - (1) Unix
  - (2) Windows
  - (3) Linux
  - (4) MS - DOS
5. वर्चुअल मेमोरी होती है -
  - (1) अत्यन्त बड़ी मुख्य मेमोरी
  - (2) अत्यन्त बड़ी द्वितीयक मेमोरी
  - (3) अत्यन्त बड़ी मेमोरी का भ्रम
  - (4) सुपर कम्प्यूटर में प्रयुक्त होने वाली मेमोरी का एक प्रकार
6. C.P.U. की प्रोसेसिंग स्पीड किस मेमोरी के नजदीक होती है?
  - (1) कैश मेमोरी
  - (2) रेन्डम ऐक्सेस मेमोरी
  - (3) रीड ओनली मेमोरी
  - (4) वर्चुअल मेमोरी
7. किसी फाईल का मानचित्रण व्यवस्थित होता है -
  - (1) वर्चुअल मेमोरी द्वारा
  - (2) फाईल मेटाडाटा द्वारा
  - (3) फाईल सिस्टम द्वारा
  - (4) उपरोक्त में से कोई नहीं

8. ....are often used where very rapid access is required, where fixed length records are used and where records are always accessed one at a time.
- (1) Direct files
  - (2) Indexed sequential files
  - (3) Indexed files
  - (4) Sequential files
9. What else is a command interpreter called?
- (1) Prompt
  - (2) Kernel
  - (3) Shell
  - (4) Command
10. Which of the following is an example of a real time operating system?
- (1) MAC
  - (2) MS - DOS
  - (3) Windows 10
  - (4) Process control
11. Which of the following is false with respect to TCP?
- (1) Connection - oriented
  - (2) Process - to - process
  - (3) Full - duplex
  - (4) Unreliable
12. Which of the following is correct IPv4 address?
- (1) 128.64.0.0
  - (2) 01.200.128.123
  - (3) 300.142.210.64
  - (4) 10110011.32.16.8
13. Protocols are set of rules to govern-
- (1) Communication
  - (2) Standard
  - (3) Metropolitan communication
  - (4) Bandwidth
14. The Internet's application layer does not include which protocol?
- (1) SMTP
  - (2) HTTP
  - (3) FTP
  - (4) UDP
8. ....फाईल वहां प्रयुक्त होती है जहां अधिक तीव्र अभिगम की आवश्यकता हो, जहां पर स्थित लम्बाई के रिकॉर्ड प्रयुक्त हों एवं जहां पर हमेशा एक बार में एक रिकॉर्ड अभिगमित किया जाता है।
- (1) Direct files
  - (2) Indexed sequential files
  - (3) Indexed files
  - (4) Sequential files
9. कमाण्ड इन्टरप्रेटर को किस अन्य नाम से भी जाना जाता है?
- (1) Prompt
  - (2) Kernel
  - (3) Shell
  - (4) Command
10. रियल टाइम ऑपरेटिंग सिस्टम का निम्न में से कौन सा उदाहरण है?
- (1) MAC
  - (2) MS - DOS
  - (3) विण्डोज 10
  - (4) प्रोसेस कंट्रोल
11. TCP के संदर्भ में निम्न में से कौन सा असत्य है?
- (1) कनेक्शन ओरियेन्टेड
  - (2) प्रोसेस-टू-प्रोसेस
  - (3) फुल-डूपलेक्स
  - (4) अविश्वसनीय
12. निम्न में से कौन सा सही IPv4 पता है?
- (1) 128.64.0.0
  - (2) 01.200.128.123
  - (3) 300.142.210.64
  - (4) 10110011.32.16.8
13. प्रोटोकॉल, जो नियमों का समूह होता है, वह किसको नियंत्रित करता है?
- (1) कम्यूनिकेशन
  - (2) मानक
  - (3) मेट्रोपोलिटियन कम्यूनिकेशन
  - (4) बैंडविड्थ
14. इन्टरनेट की अनुप्रयोग लेयर कौन से प्रोटोकॉल को सम्मिलित नहीं करता है?
- (1) SMTP
  - (2) HTTP
  - (3) FTP
  - (4) UDP

15. The FTP commands from client to server and replies from server to client are sent across the control connection in which format?
- (1) 4 - bit ASCII Format
  - (2) 7 - bit ASCII Format
  - (3) 6 - bit ASCII Format
  - (4) 8 - bit ASCII Format
16. How many bits IPv6 uses for IP address?
- (1) 64 - bits
  - (2) 128 - bits
  - (3) 32- bits
  - (4) 256 - bits
17. ....protocol provides for logical communication between application processes running on different hosts.
- (1) Transport layer
  - (2) Network layer
  - (3) Session layer
  - (4) Data link layer
18. What layer in the TCP/IP stack is equivalent to the Transport layer of the OSI Model?
- (1) Application
  - (2) Host to host
  - (3) Internet
  - (4) Network Access
19. Which of the following are True for the TCP/IP reference model?
- (i) The TCP protocol divides the large message into a sequence of packets of an IP packet.
  - (ii) The IP protocol is used to put message into the packet.
  - (iii) It is necessary for all packets in a single message to take the same route each time it is sent.
  - (iv) The packets are passed from one network to another until they reach their destination.
- (1) (i) and (iv) only
  - (2) (i), (ii) and (iv) only
  - (3) (i), (ii) and (iii) only
  - (4) All (i), (ii), (iii) and (iv)
15. FTP निर्देश क्लाइन्ट से सर्वर तथा प्रत्युत्तर में सर्वर से क्लाइन्ट को किस फॉर्मेट में कंट्रोल कनेक्शन द्वारा भेजे जाते हैं?
- (1) 4 - bit ASCII Format
  - (2) 7 - bit ASCII Format
  - (3) 6 - bit ASCII Format
  - (4) 8 - bit ASCII Format
16. IPv6, आई. पी. एड्रेस के लिए कितने बिट्स प्रयुक्त करता है?
- (1) 64 - bits
  - (2) 128 - bits
  - (3) 32- bits
  - (4) 256 - bits
17. विभिन्न hosts पर चलने वाले ऐप्लीकेशन प्रोसेसेज के मध्य तार्किक कम्यूनिकेशन.....प्रोटोकॉल द्वारा प्रदान किया जाता है।
- (1) ट्रांसपोर्ट लेयर
  - (2) नेटवर्क लेयर
  - (3) सेशन लेयर
  - (4) डाटा लिंक लेयर
18. OSI मॉडल के ट्रांसपोर्ट लेयर के समतुल्य TCP/IP स्टैक की कौनसी लेयर होती है?
- (1) Application
  - (2) Host to host
  - (3) Internet
  - (4) Network Access
19. निम्न में से TCP/IP Reference Model के लिए कौन सा कथन सत्य है?
- (i) TCP बड़े सन्देशों को IP पैकेट के क्रमिक पैकेटों में विभक्त करता है।
  - (ii) IP प्रोटोकॉल संदेशों को पैकेटों में रखता है।
  - (iii) यह आवश्यक है कि एक मैसेज के सभी पैकेट हर बार भेजते समय एक ही रूट से जावें।
  - (iv) गन्तव्य स्थान तक पहुंचने तक पैकेट एक नेटवर्क से दूसरे नेट वर्क को भेजे जाते हैं।
- (1) (i) और (iv) केवल
  - (2) (i), (ii) और (iv) केवल
  - (3) (i), (ii) और (iii) केवल
  - (4) सभी (i), (ii), (iii) और (iv)

20. Which port is used by DNS protocol?
- (1) 80
  - (2) 21
  - (3) 161
  - (4) 53
21. ....is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
- (1) Network security
  - (2) Database security
  - (3) Information security
  - (4) Physical security
22. Which of the following is an independent malicious program that does not need any host program?
- (1) Trap Doors
  - (2) Trojan Horse
  - (3) Virus
  - (4) Worm
23. A malware program that hides its true nature and reveals its designed behaviour only when activated, is called?
- (1) Trojan Horse
  - (2) Adware
  - (3) Spyware
  - (4) Worm
24. Which of the following refers to exploring the appropriate, ethical behaviours related to the online environment and digital media platform?
- (1) Cyber Law
  - (2) Cyber Ethics
  - (3) Cyber Security
  - (4) Cyber Safety
25. The.....attack is known as attack on confidentiality.
- (1) Interception
  - (2) Modification
  - (3) Fabrication
  - (4) Interruption
20. DNS प्रोटोकॉल द्वारा कौन सा पोर्ट प्रयुक्त किया जाता है?
- (1) 80
  - (2) 21
  - (3) 161
  - (4) 53
21. मूल्यवान सूचनाओं का अनाधिकृत अभिगमन, रिकॉर्डिंग, प्रकटीकरण, अथवा नष्ट करने से रक्षा करने के लिए अभ्यास एवं सावधानियों को ..... कहा जाता है।
- (1) नेटवर्क सुरक्षा
  - (2) डाटाबेस सुरक्षा
  - (3) सूचना सुरक्षा
  - (4) भौतिक सुरक्षा
22. निम्न में कौन सा स्वतंत्र दुर्भावनापूर्ण प्रोग्राम है जिसको किसी होस्ट प्रोग्राम की आवश्यकता नहीं होती है?
- (1) Trap Doors
  - (2) Trojan Horse
  - (3) Virus
  - (4) Worm
23. वह कौन सा दुर्भावनापूर्ण प्रोग्राम है, जो अपनी वास्तविक प्रकृति को छिपाये रखता है परन्तु सक्रिय होने पर उसके निर्मित व्यवहार का पता चलता है?
- (1) Trojan Horse
  - (2) Adware
  - (3) Spyware
  - (4) Worm
24. ऑनलाईन वातावरण एवं डिजिटल मीडिया प्लेटफॉर्म पर नैतिक व्यवहार द्वारा उचित तलाश को क्या कहा जाता है?
- (1) साईबर लॉ
  - (2) साईबर एथिक्स
  - (3) साईबर सिक्योरिटी
  - (4) साईबर सेफ्टी
25. ....हमले को गोपनीयता पर हमले के रूप में जाना जाता है।
- (1) Interception
  - (2) Modification
  - (3) Fabrication
  - (4) Interruption

26. This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?
- (1) SQL injection
  - (2) HTML injection
  - (3) Cross Site Scripting (XSS)
  - (4) Cross Site Request Forgery (XSRF)
27. A hacker who attacks system to conduct terrorist activities via networks or Internet pathways is called-
- (1) Ransomware
  - (2) Cyberwarfare
  - (3) Hacktivist
  - (4) Cyberterrorist
28. Information security performs which function?
- (1) Protecting the data an organization collects and uses.
  - (2) Safeguarding the organization's technology assets.
  - (3) Protecting the organization's ability to function.
  - (4) All of the above
29. DoS attacks are caused by.....
- (1) Authentication
  - (2) Alteration
  - (3) Fabrication
  - (4) Replay attacks
30. The.....method is used for hiding information.
- (1) Cryptography
  - (2) Integrity
  - (3) Steganography
  - (4) Confidentiality
31. The application of computing and network resources to try every possible password combination is called a.....
- (1) Brute force attack
  - (2) Dictionary attack
  - (3) Rainbow tables
  - (4) Social engineering
26. इस प्रकार के आक्रमण (attack) वेबसाइट के कमेंट भाग में दुर्भावनापूर्ण कोड को इन्फ्यूज कर किया जाता है। इस (attack) को क्या कहा जाता है?
- (1) SQL injection
  - (2) HTML injection
  - (3) Cross Site Scripting (XSS)
  - (4) Cross Site Request Forgery (XSRF)
27. नेटवर्क अथवा इन्टरनेट रास्तों के द्वारा सिस्टम पर आतंकवादी गतिविधियों को क्रियान्वित करने वाले को.....हैकर कहा जाता है।
- (1) रेनसमवेयर
  - (2) साईबरवॉरफेयर
  - (3) हैकटिविस्ट
  - (4) साइबरटैरिस्ट
28. सूचना सुरक्षा कौन सा कार्य सम्पादित करती है?
- (1) संख्या द्वारा संग्रहित एवं प्रयुक्त डाटा की सुरक्षा करना।
  - (2) संस्था द्वारा प्रयुक्त तकनीकी की रक्षा करना।
  - (3) संस्था के कार्य करने की क्षमता को सुरक्षा देना।
  - (4) उपरोक्त सभी
29. DoS हमले.....के कारण होते हैं।
- (1) प्रमाणीकरण
  - (2) परिवर्तन
  - (3) फेब्रिकेशन
  - (4) रीप्ले हमले
30. सूचनाओं को छुपाने के लिए .....विधि प्रयुक्त की जाती है।
- (1) क्रिप्टोग्राफी
  - (2) इन्टीग्रीटी
  - (3) स्टेगनोग्राफी
  - (4) कोनफीडेंशियैलिटी
31. कम्प्यूटिंग एवं नेटवर्क संसाधन के अनुप्रयोग जिसके द्वारा पासवर्ड के प्रत्येक समूह (combination) के लिए प्रयास किया जाता है, को.....कहते हैं।
- (1) ब्रूट फोर्स अटैक
  - (2) डिक्शनरी अटैक
  - (3) रेनबो सारणी
  - (4) सोशल अभियांत्रिकी

32. Which one is an authentication mechanism?
- (1) Something you know
  - (2) Something you have
  - (3) Something you are or can produce
  - (4) All the above
33. Which one of the following is usually used in the process of Wi – Fi hacking?
- (1) Aircrack-ng
  - (2) Wireshark
  - (3) Norton
  - (4) All of the above
34. In system hacking, which of the following is the most crucial activity?
- (1) Information gathering
  - (2) Covering tracks
  - (3) Cracking passwords
  - (4) None of the above
35. Which one is the easiest method of cracking someone's password?
- (1) By Guessing
  - (2) Brute Force attack
  - (3) Rainbow table attack
  - (4) Dictionary attack
36. Which of the following is the least secure method of authentication?
- (1) Key card
  - (2) Finger print
  - (3) Retina pattern
  - (4) Password
37. 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 attacks
  - (2) SQL injection attack
  - (3) SQL usage attack
  - (4) SQL destroyer attack
38. Which password – cracking techniques is used by hackers?
- (1) Phishing
  - (2) Social engineering
  - (3) Malware
  - (4) All of the above
32. निम्न में से प्रमाणीकरण की कार्यप्रणाली (तंत्र) कौन सी है?
- (1) Something you know
  - (2) Something you have
  - (3) Something you are or can produce
  - (4) उपरोक्त सभी
33. Wi – Fi हैकिंग प्रक्रिया में सामान्यतया से किसको प्रयुक्त किया जाता है?
- (1) Aircrack-ng
  - (2) Wireshark
  - (3) Norton
  - (4) उपरोक्त सभी
34. सिस्टम हैकिंग के दौरान निम्न में से कौन सा महत्वपूर्ण कार्य होता है?
- (1) सूचना एकत्रित करना
  - (2) कवरींग ट्रेक्स
  - (3) पासवर्ड तोड़ना
  - (4) उपरोक्त में से कोई नहीं
35. निम्न में से किसी के पासवर्ड को तोड़ने की सबसे आसान विधि कौन सी है?
- (1) अनुमान के द्वारा
  - (2) ब्रूट फोर्स अटैक द्वारा
  - (3) रेनबो सारणी अटैक द्वारा
  - (4) डिक्शनरी अटैक द्वारा
36. निम्न में से प्रमाणीकरण की सबसे कम सुरक्षित विधि कौन सी है?
- (1) की कार्ड
  - (2) फिंगरप्रिन्ट
  - (3) रेटिना पैटर्न
  - (4) पासवर्ड
37. यदि कोई आक्रामक (attack) किसी अनुप्रयोग को मैनेज करके, आक्रामक द्वारा निर्मित SQL query को execute करता है। तो इस प्रकार के attack को .....कहा जाता है।
- (1) SQL अटैक
  - (2) SQL इंजेक्शन अटैक
  - (3) SQL यूसेज अटैक
  - (4) SQL डिस्ट्रॉयर अटैक
38. हैकर के द्वारा निम्न में से पासवर्ड तोड़ने की कौन सी तकनीक प्रयुक्त की जाती है?
- (1) फिशिंग
  - (2) सोशल अभियांत्रिकी
  - (3) मालवेयर
  - (4) उपरोक्त सभी

39. ....is a weakness that can be exploited by attackers.
- (1) System with virus
  - (2) System without Firewall
  - (3) System with vulnerabilities
  - (4) System with strong password
40. Enumeration is done to gain information. Which of the following cannot be achieved using enumeration?
- (1) IP Tables
  - (2) SNMP data, if not secured appropriately
  - (3) Private chats
  - (4) List of username and password policies
41. Which of the following is not a limitation of file – based approach?
- (1) Separation and isolation of data
  - (2) Duplication of data
  - (3) Data dependence
  - (4) Sharing of data
42. .... describes what data is stored in the database and the relationship among the data.
- (1) Conceptual level
  - (2) Internal level
  - (3) External level
  - (4) Physical level
43. The overall description of the database is called-
- (1) Database mapping
  - (2) Database Instances
  - (3) Database schema
  - (4) Data Independence
44. The operation which is not considered a basic operation of relational algebra is-
- (1) Join
  - (2) Selection
  - (3) Union
  - (4) Cross product
45. Which of the following is not a record – based data model?
- (1) Relational data model
  - (2) Entity – relationship model
  - (3) Network data model
  - (4) Hierarchical data model
39. ....एक प्रकार की कमजोरी जो अटैकर द्वारा शोषित की जाती है।
- (1) सिस्टम वायरस के साथ
  - (2) सिस्टम फायरवॉल के बिना
  - (3) सिस्टम भेद्यताओं के साथ
  - (4) सिस्टम मजबूत पासवर्ड के साथ
40. सूचना प्राप्त करने के लिए परिगणना की जाती है। निम्न में से परिगणना के द्वारा किसको प्राप्त नहीं किया जा सकता है?
- (1) आई. पी. सारणी
  - (2) SNMP डाटा, यदि उचित तरह से सुरक्षित नहीं किया गया हो
  - (3) प्राइवेट चैट
  - (4) यूज़रनेम एवं पासवर्ड पॉलिसी की लिस्ट
41. निम्न में से कौनसा फाइल आधारित दृष्टिकोण का परिसीमन नहीं होगा?
- (1) डाटा का पृथक्करण एवं एकांत
  - (2) डाटा की प्रतिलिपि
  - (3) डाटा की निर्भरता
  - (4) डाटा को साझा करना
42. डाटाबेस में संग्रहित डाटा एवं उनके मध्य सम्बंध को.....लेबल द्वारा वर्णित किया जाता है।
- (1) Conceptual level
  - (2) Internal level
  - (3) External level
  - (4) Physical level
43. डाटाबेस के समस्त विवरण को .....कहा जाता है।
- (1) डाटाबेस मैपिंग
  - (2) डाटाबेस इन्सटेंसेस
  - (3) डाटाबेस स्कीमा
  - (4) डाटा इंडिपेंडेंस
44. निम्न में से Relational Algebra की कौनसी मूलभूत प्रक्रिया नहीं मानी जाती है?
- (1) जोईन
  - (2) सिलेक्शन
  - (3) यूनियन
  - (4) क्रॉस प्रोडक्ट
45. निम्न में से कौन सा रिकॉर्ड आधारित डाटा मॉडल नहीं है?
- (1) रिलेशनल डाटा मॉडल
  - (2) एन्टीटी रिलेशनल मॉडल
  - (3) नेटवर्क डाटा मॉडल
  - (4) हैरार्किकल डाटा मॉडल



46. ....is the process of maximizing the differences between members of an entity by identifying their distinguishing characteristics.
- (1) Generalization
  - (2) Composition
  - (3) Aggregation
  - (4) Specialization
47. A relation is in....., if and only if, every determinant is a candidate key.
- (1) Boyce-Codd Normal Form
  - (2) Third Normal Form
  - (3) First Normal Form
  - (4) Second Normal Form
48. What is a relational calculus?
- (1) It is a kind of procedural language
  - (2) It is a non – procedural language
  - (3) It is a high level language
  - (4) It is a data definition language
49. The.....of a relation is the number of tuples it contains.
- (1) Degree
  - (2) Domain
  - (3) Cardinality
  - (4) Attribute
50. A table is in 3NF, if it is in 2NF and if it has no.....
- (1) Functional Dependencies
  - (2) Transitive Dependencies
  - (3) Trivial Functional Dependency
  - (4) Multivalued Dependencies
51. In cryptography, what is cipher?
- (1) Algorithm for performing encryption and decryption
  - (2) Encrypted message
  - (3) Both algorithm for performing encryption and decryption and encrypted message
  - (4) Decrypted message
52. DES Follows-
- (1) Hash algorithm
  - (2) Caesars cipher
  - (3) Feistel cipher structure
  - (4) SP Networks
46. किसी इकाई के विभिन्न गुणों में अन्तर को पहचानते हुए उसके विभिन्न सदस्यों के मध्य अधिकतम अन्तर करने को.....कहा जाता है।
- (1) सामान्यीकरण
  - (2) संघटन
  - (3) एकत्रीकरण
  - (4) विशेषज्ञता
47. एक सम्बन्ध ..... में होगा, यदि केवल उसका प्रत्येक निर्धारक एक कैंडिडेट कुंजी हो।
- (1) Boyce-Codd नॉर्मल फॉर्म
  - (2) तृतीय नॉर्मल फॉर्म
  - (3) प्रथम नॉर्मल फॉर्म
  - (4) द्वितीय नॉर्मल फॉर्म
48. रिलेशनल केलकुलस क्या है?
- (1) प्रक्रियात्मक भाषा का एक प्रकार
  - (2) गैर प्रक्रियात्मक भाषा का एक प्रकार
  - (3) एक उच्च स्तरीय भाषा
  - (4) एक डाटा .डेफिनेशन भाषा
49. किसी संबंध की ..... इसमें शामिल टपल्स की संख्या से है।
- (1) डिग्री
  - (2) डोमेन
  - (3) कार्डिनैलिटी
  - (4) एट्रीब्यूट
50. एक सारणी 3NF में होगी, यदि वह 2NF में हो एवं उसमें.....नहीं हो।
- (1) Functional Dependencies
  - (2) Transitive Dependencies
  - (3) Trivial Functional Dependency
  - (4) Multivalued Dependencies
51. क्रिप्टोग्राफी के संन्दर्भ में साईफर क्या है?
- (1) Encryption एवं decryption को perform करने के लिए एल्गोरिथम
  - (2) इनक्रेप्टेड संदेश
  - (3) Encryption एवं decryption को perform करने की एल्गोरिथम एवं इनक्रेप्टेड संदेश दोनों
  - (4) डिक्रिप्टेड संदेश
52. DES अनुसरण करता है –
- (1) हैश एल्गोरिथम
  - (2) Caesars साईफर
  - (3) फिस्टियल साईफर संरचना
  - (4) SP नेटवर्क

53. Till when was the RC4 algorithm kept a secret?
- (1) 1990
  - (2) 1992
  - (3) 1996
  - (4) 1994
54. Suppose in RSA,  $p = 11$  and  $q = 19$ , taking  $e = 17$ , apply RSA algorithm to encrypt a message  $M = 5$  and find the cipher text
- (1)  $C = 80$
  - (2)  $C = 102$
  - (3)  $C = 64$
  - (4)  $C = 13$
55. PKI stands for.....
- (1) Proxy Key Infrastructure
  - (2) Public Key Infrastructure
  - (3) Public Kinetic Infrastructure
  - (4) Private Key Infrastructure
56. Digital signature is created and verified using .....
- (1) Program
  - (2) Graphical coding
  - (3) HTML
  - (4) Cryptography
57. Which of them is not a major way of stealing e-mail information?
- (1) Stealing cookies
  - (2) Reverse Engineering
  - (3) Password Phishing
  - (4) Social Engineering
58. When a hash function is used to provide message authentication, the hash function value is referred to as -
- (1) Message Field
  - (2) Message Digest
  - (3) Message Score
  - (4) Message Leap
59. Another name for message authentication codes is-
- (1) Cryptographic codebreak
  - (2) Cryptographic codesum
  - (3) Cryptographic checksum
  - (4) Cryptographic checkbreak
53. RC4 एल्गोरिथम को कब तक गुप्त रखा गया था?
- (1) 1990
  - (2) 1992
  - (3) 1996
  - (4) 1994
54. मान लीजिए RSA में  $p = 11$  और  $q = 19$  है,  $e = 17$  लेते हुए,  $M = 5$  संदेश को एन्क्रिप्ट करने के लिए, RSA एल्गोरिथम लागू करें और साइफर टेक्स्ट खोजें -
- (1) सी = 80
  - (2) सी = 102
  - (3) सी = 64
  - (4) सी = 13
55. PKI का अभिप्राय है -
- (1) Proxy Key Infrastructure
  - (2) Public Key Infrastructure
  - (3) Public Kinetic Infrastructure
  - (4) Private Key Infrastructure
56. डिजिटल हस्ताक्षर ..... के द्वारा निर्मित एवं सत्यापित किये जाते हैं।
- (1) प्रोग्राम
  - (2) ग्राफिकल कोडिंग
  - (3) HTML
  - (4) क्रिप्टोग्राफी
57. E-mail सूचना को चुराने का निम्न में से कौनसा मुख्य (major) तरीका नहीं है?
- (1) कुकीज़ चुराना
  - (2) रिवर्स अभियांत्रिकी
  - (3) पासवर्ड फिशिंग
  - (4) सोशल अभियांत्रिकी
58. संदेश के प्रमाणीकरण के लिए जब हैश फलन को प्रयुक्त किया जाता है तब हैश फलन मान को सन्दर्भित (referred) किया जाता है -
- (1) संदेश क्षेत्र
  - (2) संदेश डाईजेस्ट
  - (3) संदेश स्कोर
  - (4) संदेश लीप
59. संदेश प्रमाणीकरण कोड को ..... नाम से भी जाना जाता है।
- (1) क्रिप्टोग्राफिक कोडब्रेक
  - (2) क्रिप्टोग्राफिक कोडसम
  - (3) क्रिप्टोग्राफिक चेकसम
  - (4) क्रिप्टोग्राफिक चेकब्रेक

60. What are the different ways to classify an Intrusion Detection System (IDS)?
- (1) Zone based
  - (2) Host and network based
  - (3) Network and zone based
  - (4) Level based
61. Software that enables a user to obtain secret information about another computer's activities -
- (1) Malware
  - (2) Adware
  - (3) Spyware
  - (4) Trackware
62. Which of the following malware do not replicate or reproduce through infection?
- (1) Worms
  - (2) Trojans
  - (3) Viruses
  - (4) Rootkits
63. ....field in the "Portable Executable" needs to be executed first by windows executable for addressing intrusion.
- (1) Starting point
  - (2) Point of origin
  - (3) Thread origination point
  - (4) Entry point
64. A program that deletes all the data from a computer is-
- (1) Virus
  - (2) Malware
  - (3) Adware
  - (4) Sweeper
65. The key benefits of malware analysis is/are-
- (1) Assesses the damage from a security threat
  - (2) Identify the source of attack
  - (3) Identify the vulnerability of the malware
  - (4) All of the above
60. इन्ट्रूशन डिटेक्शन सिस्टम (IDS) को वर्गीकरण करने के विभिन्न तरीके कौन से हैं?
- (1) ज़ोन आधारित
  - (2) Host एवं नेटवर्क आधारित
  - (3) नेटवर्क एवं ज़ोन आधारित
  - (4) स्तर आधारित
61. वह सॉफ्टवेयर जो प्रयोक्ता को दूसरे कम्प्यूटर की गतिविधियों की गोपनीय सूचना को प्राप्त करने में सहायक होता है -
- (1) मालवेयर
  - (2) ऐडवेयर
  - (3) स्पाईवेयर
  - (4) ट्रैकवेयर
62. निम्न में से कौन सा मालवेयर संक्रमण के द्वारा पुनः दोहराना अथवा पुनःनिर्मित नहीं होता है?
- (1) Worms
  - (2) Trojans
  - (3) Viruses
  - (4) Rootkits
63. "पोर्टेबल एक्जीक्यूटेबल" में .....फील्ड को घुसपैठ को संबोधित करने के लिए पहले विंडोज़ एक्जीक्यूटेबल द्वारा निष्पादित करने की आवश्यकता है।
- (1) Starting point
  - (2) Point of origin
  - (3) Thread origination point
  - (4) Entry point
64. वह प्रोग्राम जो कम्प्यूटर पर से सभी डाटा को नष्ट करता है-
- (1) Virus
  - (2) Malware
  - (3) Adware
  - (4) Sweeper
65. मालवेयर विश्लेषण के मुख्य लाभ हैं -
- (1) सुरक्षा धमकी के नुकसान का आकलन करना
  - (2) आक्रमण के स्रोत की पहचान करना
  - (3) मालवेयर की भेद्यताओं की पहचान करना
  - (4) उपरोक्त सभी

66. Which one of the following is/are a feature of APK Tool?
- (1) Rebuilding decoded resources back to binary
  - (2) Helping with repetitive tasks
  - (3) Organizing and handling APKs that depend on framework resources
  - (4) All the above
67. Which component of android architecture provides an abstraction layer between hardware and other components?
- (1) Linux kernel
  - (2) Application framework
  - (3) Android Runtime
  - (4) Applications
68. The sandbox is related to which type of malware analysis?
- (1) Static malware analysis
  - (2) Dynamic malware analysis
  - (3) Both static and dynamic malware analysis
  - (4) None of above
69. Which of the following static code analysis tool perform language specific security analysis?
- (1) PVS – studio
  - (2) Deepsourc
  - (3) RIPS Technologies
  - (4) None of these
70. Which of the following is/are the advantages of virtualization?
- (1) Support cross – platform analysis
  - (2) Provide system protection
  - (3) Easily creates ideal testing conditions
  - (4) All the above
71. Machine learning is a subset of.....
- (1) Data learning
  - (2) Artificial Intelligence
  - (3) Deep learning
  - (4) None of the above
66. निम्न में से APK Tool की विशेषताएं कौन सी हैं?
- (1) Decoded स्रोत को पुनः बाइनरी में निर्मित करना
  - (2) रैपेटिटिव कार्य में सहायता करना
  - (3) फ्रेमवर्क स्रोत पर निर्भर APKs को व्यवस्थित करना एवं संभालना
  - (4) उपरोक्त सभी
67. Android संरचना का कौन सा घटक हार्डवेयर एवं अन्य घटकों के मध्य abstraction layer प्रदान करता है?
- (1) Linux kernel
  - (2) Application framework
  - (3) Android Runtime
  - (4) Applications
68. Sandbox का सम्बन्ध किस प्रकार के मालवेयर विश्लेषण से है?
- (1) स्थिर मालवेयर विश्लेषण
  - (2) गतिशील मालवेयर विश्लेषण
  - (3) स्थिर एवं गतिशील मालवेयर विश्लेषण दोनों
  - (4) उपरोक्त में से कोई नहीं
69. निम्न में से कौन सा स्थिर कोड विश्लेषण टूल, भाषा विशेष की सुरक्षा विश्लेषण को संपादित करता है?
- (1) PVS - studio
  - (2) Deepsourc
  - (3) RIPS Technologies
  - (4) उपरोक्त में से कोई नहीं
70. निम्न में से आभासीकरण के कौन से लाभ हैं?
- (1) Cross – platform विश्लेषण का समर्थन
  - (2) सिस्टम प्रोटेक्शन प्रदान करना
  - (3) आदर्श टेस्टिंग शर्तों को आसानी से निर्मित करना
  - (4) उपरोक्त सभी
71. Machine learning किसका उपसमुच्चय (subset) है?
- (1) Data learning
  - (2) Artificial Intelligence
  - (3) Deep learning
  - (4) उपरोक्त में से कोई नहीं

72. Among the following option identify the one which is not a type of learning?
- (1) Supervised learning
  - (2) Unsupervised learning
  - (3) Semi unsupervised learning
  - (4) Reinforcement learning
73. ....bytes size data is called Big Data.
- (1) Tera
  - (2) Giga
  - (3) Peta
  - (4) Meta
74. The decision tree algorithm reaches its destination using-
- (1) Single Test
  - (2) Two Test
  - (3) Sequence of Test
  - (4) No test
75. What is the disadvantage of decision trees?
- (1) Factor analysis
  - (2) Decision trees are robust to outliers
  - (3) Decision trees are prone to be overfit
  - (4) All of the above
76. Identify the different features of Big data analytics-
- (1) Open source
  - (2) Data Recovery
  - (3) Scalability
  - (4) All of the above
77. How many V's of Big Data?
- (1) 5
  - (2) 4
  - (3) 2
  - (4) 3
78. Amongst which of the following is/are not Big Data Technologies?
- (1) Apache Hadoop
  - (2) Apache Pytarch
  - (3) Apache Kafka
  - (4) Apache Spark
72. निम्न विकल्पों में कौन सा विकल्प सीखने का विकल्प नहीं है?
- (1) Supervised learning (निगरानी सीखना)
  - (2) Unsupervised learning (गैरनिगरानी सीखना)
  - (3) Semi unsupervised learning (अर्ध गैरनिगरानी सीखना)
  - (4) Reinforcement learning (सुदृढ़ीकरण सीखना)
73. ....बाइट आकार के डेटा को बिग डेटा कहा जाता है।
- (1) टेरा
  - (2) गीगा
  - (3) पेटा
  - (4) मेटा
74. Decision tree एल्गोरिथम अपने गन्तव्य तक ..... प्रयुक्त करके पहुंचती है।
- (1) Single Test
  - (2) Two Test
  - (3) Sequence of Test
  - (4) No test
75. Decision trees के कौन से disadvantage हैं?
- (1) फैक्टर विश्लेषण
  - (2) Decision tree बाहरी कारकों के कारणों के प्रति मजबूत
  - (3) Decision tree overfit की ओर प्रवृत्त
  - (4) उपरोक्त सभी
76. बिग डाटा विश्लेषक की विशेषताओं को पहिचानिए -
- (1) खुला स्रोत
  - (2) डाटा रिकवरी
  - (3) स्केलेबिलिटी
  - (4) उपरोक्त सभी
77. Big डाटा के कितने V's होते हैं?
- (1) 5
  - (2) 4
  - (3) 2
  - (4) 3
78. निम्न में से कौन सी Big Data तकनीकी नहीं है?
- (1) Apache Hadoop
  - (2) Apache Pytarch
  - (3) Apache Kafka
  - (4) Apache Spark

79. All of the following accurately describe Hadoop, EXCEPT-
- (1) Open source
  - (2) Distributed computing approach
  - (3) Java - based
  - (4) Real time
80. Which of the following is not a supervised learning?
- (1) Naive Bayesion
  - (2) Linear Regression
  - (3) PCA
  - (4) Decision Tree
81. What is the primary goal of an Ethical Hacker?
- (1) Determining return on investment for security measures
  - (2) Avoiding detection
  - (3) Resolving security vulnerabilities
  - (4) Testing security controls
82. ARP poisoning is also known as-
- (1) ARP poison routing
  - (2) ARP cache poisoning
  - (3) ARP spoofing
  - (4) All of the above
83. What is the preferred communication method used with systems on a bot-net?
- (1) IRC
  - (2) E - mail
  - (3) ICMP
  - (4) TFTP
84. The maximum length of an SSID is.....
- (1) 64 characters
  - (2) 16 characters
  - (3) 32 characters
  - (4) 8 characters
85. An Ethical Hacker is asked to perform a penetration test for a client and all he has received is a URL. What kind of test is this?
- (1) White box penetration Test
  - (2) Black Box penetration Test
  - (3) Black hat hacking test
  - (4) None of these
86. Which of the following is/are the type of firewall?
- (1) Packet filtering Firewall
  - (2) Dual homed gateway Firewall
  - (3) Screen host firewall
  - (4) Dual host firewall
79. निम्न में से Hadoop का कौन सही तरीके से वर्णन नहीं करता है?
- (1) ओपन सोर्स
  - (2) डिस्ट्रीब्यूटेड कम्प्यूटिंग अप्रोच
  - (3) जावा-आधारित
  - (4) रियल-टाईम
80. निम्न में से कौन सा supervised learning नहीं है?
- (1) Naive Bayesion
  - (2) लिनियर रिग्रेशन
  - (3) PCA
  - (4) Decision Tree
81. Ethical Hacker का मुख्य उद्देश्य क्या होता है?
- (1) सुरक्षा पैमाने में निवेश के रिटर्न को निर्धारित करना
  - (2) Avoiding detection
  - (3) सुरक्षा भेद्यताओं को हल करना
  - (4) सुरक्षा कंट्रोल का परीक्षण करना
82. ARP poisoning को और क्या कहा जाता है?
- (1) ARP poison routing
  - (2) ARP cache poisoning
  - (3) ARP spoofing
  - (4) उपरोक्त सभी
83. bot-net पर सिस्टमों के द्वारा पसंदीदा कम्प्यूनिकेशन विधि कौन सी है?
- (1) IRC
  - (2) E - mail
  - (3) ICMP
  - (4) TFTP
84. एक SSID की अधिकतम लंबाई.....होती है।
- (1) 64 वर्ण
  - (2) 16 वर्ण
  - (3) 32 वर्ण
  - (4) 8 वर्ण
85. Ethical Hacker को क्लाइन्ट के लिए penetration test करने के लिए कहा जाता है एवं उसको एक URL प्राप्त होता है। यह किस प्रकार का परीक्षण है?
- (1) White box penetration Test
  - (2) Black Box penetration Test
  - (3) Black hat hacking test
  - (4) उपरोक्त में से कोई नहीं
86. निम्न में से Firewall का प्रकार कौन सा है?
- (1) पैकेट फिल्टरिंग फायरवॉल
  - (2) ड्यूल होम्ड गेटवे फायरवॉल
  - (3) स्क्रीन होस्ट फायरवॉल
  - (4) ड्यूल होस्ट फायरवॉल

87. The term "Zombie Devices" is related to which type of DoS (Denial Of Service) attack?
- (1) Application – layer Flood attack
  - (2) Distributed denial of service attack
  - (3) Unintended denial of service attack
  - (4) None of these
88. Wired Equivalent Privacy (WEP) protocol uses encryption at which layer?
- (1) Network layer
  - (2) Session layer
  - (3) Transport layer
  - (4) Data link layer
89. What is botnets?
- (1) Attackers build a network of hacked machine
  - (2) A type of DoS (Denial Of Service)
  - (3) A type of antivirus
  - (4) None of these
90. Who is also known as "Crackers" in Ethical Hacking?
- (1) White Hat Hackers
  - (2) Black Hat Hackers
  - (3) Grey Hat Hackers
  - (4) Red Hat Hackers
91. The NTSC stands for –
- (1) National Telescope Standard Committee
  - (2) National Television Standard Committee
  - (3) National Talent Search Committee
  - (4) None of the above
92. The specified frame rate as per PAL standard is –
- (1) 25 FPS
  - (2) 30 FPS
  - (3) 80 FPS
  - (4) 36 FPS
93. A video consists of sequence of .....
- (1) Frames
  - (2) Signals
  - (3) Packets
  - (4) Slots
87. "Zombie Devices" पद किस प्रकार/कौनसे DoS (Denial Of Service) attack से संबंधित है?
- (1) एल्पीकेशन लेयर फ्लड अटैक
  - (2) डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस अटैक
  - (3) अनईन्टेड डिनायल ऑफ सर्विस अटैक
  - (4) उपरोक्त में से कोई नहीं
88. WEP (वायर्ड इक्विवेलेन्ट प्राइवैसी) प्रोटोकॉल encryption का किस लेयर पर उपयोग करता है?
- (1) नेटवर्क लेयर
  - (2) सेशन लेयर
  - (3) ट्रांसपोर्ट लेयर
  - (4) डाटा लिंक लेयर
89. Botnets क्या है?
- (1) Attackers द्वारा hacked मशीनों का एक नेटवर्क बनाना
  - (2) DoS का एक प्रकार (Denial Of Service)
  - (3) Antivirus का एक प्रकार
  - (4) उपरोक्त में से कोई नहीं
90. Ethical Hacking में "Crackers" के नाम से भी कौन जाने जाते हैं?
- (1) White Hat Hackers
  - (2) Black Hat Hackers
  - (3) Grey Hat Hackers
  - (4) Red Hat Hackers
91. एन.टी.एस.सी. का क्या अर्थ है?
- (1) नेशनल टेलिस्कोप स्टैंडर्ड कमेटी
  - (2) नेशनल टेलीविज़न स्टैंडर्ड कमेटी
  - (3) नेशनल टैलेंट सर्च कमेटी
  - (4) उपरोक्त में कोई भी नहीं
92. पी.ए.एल. मानकों के अनुरूप निर्दिष्ट फ्रेम दर क्या है?
- (1) 25 FPS
  - (2) 30 FPS
  - (3) 80 FPS
  - (4) 36 FPS
93. एक वीडियो में निम्न में से किस का अनुक्रम होता है?
- (1) फ्रेम्स
  - (2) सिगनल
  - (3) पैकेट
  - (4) स्लोट

94. Which amongst the following techniques are useful for detection of a manipulated image?
- (1) The analysis of abrupt changes in the outline of an object in the image
  - (2) Checking the exif data of the image
  - (3) None of these
  - (4) Both (1) and (2)
95. Motion blurring in the video is due to –
- (1) Movement of camera
  - (2) Motion of vehicle
  - (3) Fluctuation in electricity
  - (4) Issue in camera lens
96. Which of the following is the first and foremost step in image processing?
- (1) Image acquisition
  - (2) Segmentation
  - (3) Image enhancement
  - (4) Image restoration
97. A video digitally edited to replace original subject with another subject is termed as –
- (1) Digitally fake
  - (2) Metadata
  - (3) Deep fake
  - (4) Animated Video
98. The properties of an optical image can be altered by –
- (1) Selectively adding spatial filter
  - (2) Selectively removing certain spatial frequencies
  - (3) Both (1) and (2)
  - (4) None of the above
99. The JPEG stand for –
- (1) Joint People Expert Group
  - (2) Joint Photographic Expert Group
  - (3) Joint Principal Expert Group
  - (4) None of the above
100. Which amongst the following are open source tools for enhancement of voice samples?
- (1) Goldwave
  - (2) Audacity
  - (3) Praat
  - (4) All of the above
94. निम्नलिखित में से किस विधि द्वारा हेर फेर की गई छवि का पता लगाया जाता है?
- (1) छवि में किसी वस्तु की रूप रेखा में अचानक परिवर्तन का विश्लेषण करके
  - (2) छवि के exif डाटा की जांच करके
  - (3) इनमें से कोई नहीं
  - (4) उपरोक्त (1) व (2)
95. वीडियो में मोशन ब्लरिंग क्यों होता है?
- (1) कैमरे की गति से
  - (2) वाहन की गति से
  - (3) बिजली की अस्थिरता के कारण
  - (4) कैमरे के लेंस में इश्यू
96. निम्नलिखित में से कौन सा इमेज प्रोसेसिंग में पहला और सबसे महत्वपूर्ण कदम है?
- (1) इमेज एक्वीजीशन
  - (2) सेगमेंटेशन
  - (3) इमेज एनहांसमेंट
  - (4) इमेज रेस्टोरेशन
97. मूल विषय को किसी अन्य विषय से बदलने के लिए डिजिटल रूप से संपादित वीडियो को क्या कहा जाता है?
- (1) डिजिटल रूप से नकली
  - (2) मेटा डेटा
  - (3) डीप फेक
  - (4) एनिमेटेड वीडियो
98. एक ऑप्टिकल छवि के गुणों को बदला जा सकता है –
- (1) चुनिंदा स्थानिक फिल्टर जोड़कर
  - (2) कुछ स्थानिक आवृत्तियों को चुनिंदा रूप से हटा कर
  - (3) उपरोक्त (1) व (2)
  - (4) उपरोक्त में से कोई भी नहीं
99. JPEG शब्द का अर्थ है –
- (1) Joint People Expert Group
  - (2) Joint Photographic Expert Group
  - (3) Joint Principal Expert Group
  - (4) उपरोक्त में से कोई भी नहीं
100. निम्नलिखित में से आवाज की एनहांसमेंट में किन ओपन सोर्स सॉफ्टवेयर का इस्तेमाल किया जाता है?
- (1) गोल्ड वेव
  - (2) औडीसिटी
  - (3) प्राट
  - (4) उपरोक्त सभी



101. Which amongst the following chipsets cannot be used in Apple devices?  
 (1) Kirin  
 (2) Tensor  
 (3) Exynos  
 (4) All the above
102. A file system Dump is –  
 (1) Hybrid of logical extraction and scroll analysis  
 (2) Hybrid of physical extraction and logical extraction  
 (3) Logical extraction  
 (4) Only physical extraction
103. Each mobile handset is uniquely identified by –  
 (1) IMEI number  
 (2) Model number  
 (3) Name of the device  
 (4) Modal Type
104. The deleted data from any mobile phone can be extracted with a method –  
 (1) Logical Extraction  
 (2) Scroll Analysis  
 (3) Physical Extraction  
 (4) File system Extraction
105. The term GSM and CDMA denotes –  
 (1) Network Types  
 (2) Sim Cards  
 (3) Temporal analysis  
 (4) None of the above
106. An open source mobile operating system based on Linux 2.6 kernel and is owned by Google –  
 (1) Symbian  
 (2) Android  
 (3) IOS  
 (4) None of the above
107. The use of Faraday bag for keeping mobile phone in digital forensic laboratory is recommended to isolate from –  
 (1) Electrostatic radiation  
 (2) Static current  
 (3) Network  
 (4) All the above
101. निम्नलिखित में से कौन सा चिपसेट एप्पल डिवाइसेस में इस्तेमाल नहीं किया जा सकता है?  
 (1) किरिन (Kirin)  
 (2) टेन्सन (Tensor)  
 (3) एक्सीनॉस (Exynos)  
 (4) उपरोक्त सभी
102. फाइल सिस्टम डम्प का अभिप्राय क्या है?  
 (1) लोजिकल एक्सट्रैक्शन व स्कॉल एनालिसिस का हाइब्रिड  
 (2) फिजिकल एक्सट्रैक्शन व लोजिकल एक्सट्रैक्शन का हाइब्रिड  
 (3) लोजिकल एक्सट्रैक्शन  
 (4) केवल फिजिकल एक्सट्रैक्शन
103. प्रत्येक मोबाइल हैंडसेट के लिये अद्वितीय क्या है?  
 (1) आइ.एम.ई.आइ. नम्बर  
 (2) मॉडल नम्बर  
 (3) डिवाइस का नाम  
 (4) मॉडल टाईप
104. मोबाइल फोन में नष्ट किये डाटा को किस विधि द्वारा निष्कर्षण से पुनः प्राप्त किया जा सकता है?  
 (1) लोजिकल निष्कर्षण  
 (2) स्कॉल विश्लेषण  
 (3) फिजिकल निष्कर्षण  
 (4) फाइल सिस्टम निष्कर्षण
105. जी.एस.एम व सी.डी.एम.ए. का क्या तात्पर्य है?  
 (1) नेटवर्क प्रकार  
 (2) सिम कार्ड  
 (3) टेम्पोरल विश्लेषण  
 (4) उपरोक्त में से कोई भी नहीं
106. एक ओपन सोर्स मोबाइल ओपरेटिंग सिस्टम जो लाइनेक्स 2.6 कर्नेल पर आधारित व इसका स्वामित्व गूगल के पास है –  
 (1) सिम्बियन  
 (2) एंड्रॉयड  
 (3) आई ओ एस  
 (4) उपरोक्त में से कोई भी नहीं
107. डिजिटल फॉरेंसिक लेबोरेटरी में फ़ैराडे बैग का प्रयोग करके मोबाइल फोन को अलग रखने की सलाह क्यों दी जाती है?  
 (1) इलेक्ट्रोस्टैटिक विकिरणों से बचाव हेतू  
 (2) स्टैटिक करंट से बचाव हेतू  
 (3) नेटवर्क से बचाव हेतू  
 (4) उपरोक्त सभी

108. A tool used for jailbreak supported Iphone is called as –
- (1) Chakra 1n
  - (2) Chimera
  - (3) Pangu 8
  - (4) All of the above
109. Emergency download mode is a powerful technique to bypass locked mobile devices where USB debugging is –
- (1) Enabled
  - (2) Not enabled
  - (3) Both (1) and (2)
  - (4) None of the above
110. A software capable of image recognition engine, can understand the contents of images and classifies them according to categories like drugs, weapon and people is known as –
- (1) MSAB ive
  - (2) MSAB Santoku
  - (3) MSAB XRY
  - (4) All the above
111. A SAM file in windows computer specifically stores –
- (1) User Password
  - (2) Registry
  - (3) Carved Data
  - (4) All of the above
112. The hash function SHA – 1 has –
- (1) 128 bytes
  - (2) 30 bytes
  - (3) 20 bytes
  - (4) 10 bytes
113. What types of signals can network cameras transmit / receive using a single network cable?
- (1) Video
  - (2) Audio
  - (3) PTZ controls
  - (4) All of the above
114. The vulnerability in the system is related with –
- (1) A cyber attack
  - (2) Weakness in the system
  - (3) Both (1) and (2)
  - (4) None of the above
108. निम्नलिखित में से किस उपकरण का इस्तेमाल जेल ब्रेक समर्थित Iphone के लिये किया जा सकता है?
- (1) चक्रा 1n
  - (2) काइमेरा
  - (3) पांगू 8
  - (4) उपरोक्त सभी
109. आपातकालीन डाउनलोड मोड लॉकड मोबाइल उपकरणों को बायपास करने के लिये एक प्रबल तकनीक है जहां यू एस बी डिबगिंग –
- (1) सक्षम (Enabled)
  - (2) सक्षम नहीं (Not Enabled)
  - (3) उपरोक्त (1) व (2)
  - (4) उपरोक्त में से कोई भी नहीं
110. छवि पहचान इंजन में सक्षम एक सॉफ्टवेयर छवियों की सामग्री को समझ सकता है और उन्हें विभिन्न श्रेणियों जैसे ड्रग्स हथियार और लोगों के अनुसार वर्गीकृत कर सकता है, कहलाता है –
- (1) एम एस ए बी ive
  - (2) एम एस ए बी Santoku
  - (3) एम एस ए बी XRY
  - (4) उपरोक्त सभी
111. विंडोज कम्प्यूटर में एक सैम फाइल विशेष रूप से स्टोर करती है –
- (1) उपयोगकर्ता पासवर्ड
  - (2) रजिस्ट्री
  - (3) कार्वेड डाटा
  - (4) उपरोक्त सभी
112. हैश फंक्शन SHA – 1 में है –
- (1) 128 बाइट्स
  - (2) 30 बाइट्स
  - (3) 20 बाइट्स
  - (4) 10 बाइट्स
113. एक नेटवर्क केबल का उपयोग करके नेटवर्क कैमरे किस प्रकार के सिग्नल संचारित/प्राप्त कर सकते हैं?
- (1) विडियो
  - (2) ऑडियो
  - (3) पी टि जेड कंट्रोल्स
  - (4) उपरोक्त सभी
114. सिस्टम में वल्नेरेबिलिटी से सम्बंधित है –
- (1) एक साइबर हमला
  - (2) सिस्टम में कमजोरी
  - (3) (1) व (2) दोनों
  - (4) उपरोक्त में से कोई भी नहीं

115. Digital forensics consists of –  
 (1) Computer Forensics  
 (2) Mobile Forensic  
 (3) Cloud Forensics  
 (4) All of the above
116. Who invented computer?  
 (1) Charles William  
 (2) Alan Turing  
 (3) Charles Babbage  
 (4) None of the above
117. The techniques used for computer forensics investigation –  
 (1) Cross – drive analysis  
 (2) Live analysis  
 (3) Deleted file analysis  
 (4) All of the above
118. Write blockers are used to prevent writings on –  
 (1) Suspect drive  
 (2) Destination drive  
 (3) Both (1) and (2)  
 (4) None of the above
119. The file system found in DVR is –  
 (1) HFS  
 (2) YAFFS  
 (3) APFS  
 (4) FAT32
120. The FTK imager is used to –  
 (1) Image the drive  
 (2) Preview the data  
 (3) RAM capture  
 (4) All of the above
121. If a sample call cell ID is 404601070046655 Match the following–  
 (A) Mobile Network Code (P) 404  
 (B) Mobile Country Code (Q) 60  
 (C) Location Area Code (R) 46655  
 (D) Cell ID (S) 10700  
 (1) A – S, B – Q, C – P, D – R  
 (2) B – P, A – Q, C – R, D – S  
 (3) B – P, A – S, C – Q, D – R  
 (4) A – Q, B – P, C – S, D – R
115. डिजिटल फॉरेंसिक्स में सम्मिलित है –  
 (1) कम्प्यूटर फॉरेंसिक  
 (2) मोबाइल फॉरेंसिक  
 (3) क्लाउड फॉरेंसिक  
 (4) उपरोक्त सभी
116. कम्प्यूटर का अविष्कार किसने किया?  
 (1) चार्ल्स विलियम  
 (2) एलन ट्यूरिंग  
 (3) चार्ल्स बैबेज  
 (4) उपरोक्त में से कोई भी नहीं
117. कम्प्यूटर फॉरेंसिक जाँच के लिए प्रयोग में लाई जाने वाली विधियाँ –  
 (1) क्रॉस – ड्राइव विश्लेषण  
 (2) लाइव विश्लेषण  
 (3) डिलीट की गई फाइल का विश्लेषण  
 (4) उपरोक्त सभी
118. राइट ब्लॉकर्स का उपयोग ..... पर लिखने से बचाव के लिये किया जाता है।  
 (1) सॉन्डिथ ड्राइव  
 (2) डेस्टिनेशन ड्राइव  
 (3) उपरोक्त (1) व (2)  
 (4) उपरोक्त में से कोई भी नहीं
119. डी.वी.आर. में पाया जाने वाला फाइल सिस्टम है –  
 (1) एच.एफ.एस.  
 (2) वाइ.ए.एफ.एफ.एस.  
 (3) ए.पी.एफ.एस.  
 (4) एफ.ए.टी. 32
120. एफ.टी.के. इमेजर का प्रयोग किया जाता है –  
 (1) इमेज ड्राइव बनाने के लिए  
 (2) डेटा का प्राभ्यास  
 (3) आर ए एम कैप्चर  
 (4) उपरोक्त सभी
121. यदि एक नमूना कॉल का सैल ID 404601070046655 है, तो निम्नलिखित का मिलान करते हुए सही क्रम पहचाने –  
 (A) मोबाइल नेटवर्क कोड (P) 404  
 (B) मोबाइल कंट्री कोड (Q) 60  
 (C) लोकेशन एरिया कोड (R) 46655  
 (D) सैल आई डी (S) 10700  
 (1) A – S, B – Q, C – P, D – R  
 (2) B – P, A – Q, C – R, D – S  
 (3) B – P, A – S, C – Q, D – R  
 (4) A – Q, B – P, C – S, D – R

122. Which of the following app does not provide virtual number?  
 (1) Text now  
 (2) Text plus  
 (3) 2nd line  
 (4) Signal
123. The VOIP service that does not require any e-mail or phone number for registration to use is –  
 (1) Signal  
 (2) Whatsapp  
 (3) Skype  
 (4) Wickrme
124. When a suspect is using TOR, then on analysis of IPDR, how can we confirm for the same?  
 (1) By analysing the source port  
 (2) By analysing the destination port  
 (3) By analysing the public IP  
 (4) All of the above
125. The term IPDR stands for –  
 (1) Intellectual Property Detail Record  
 (2) International Public Domain Record  
 (3) Internet Protocol Detail Record  
 (4) None of the above
126. The best indicator of phone/s being used in JAIL is –  
 (1) Multiple IMEI and many cell ID in CDR  
 (2) Many cell ID and multiple IMSI in CDR  
 (3) Both (1) and (2)  
 (4) None of the above
127. 1<sup>st</sup> 6 – 8 digits of IMEI number is called as –  
 (1) TAC  
 (2) MAC  
 (3) IPMAC  
 (4) IPV<sub>6</sub> MAC
128. The zero day attack occurs –  
 (1) On the day the application or OS is released  
 (2) Before a patch is available  
 (3) Before the vendor is aware of vulnerability  
 (4) Both (2) and (3)
122. निम्नलिखित एप्प में से कौन वर्चुअल नम्बर प्रदान नहीं करता है?  
 (1) टेक्सट नाओ  
 (2) टेक्सट प्लस  
 (3) 2nd लाइन  
 (4) सिग्नल
123. किस वी.ओ.आइ.पी. सेवा के उपयोग हेतु पंजीकरण के लिये फोन नम्बर एवं ई-मेल की आवश्यकता नहीं है –  
 (1) सिग्नल  
 (2) वॉट्सैप  
 (3) स्काइप  
 (4) विकरमी
124. जब कोई संदिग्ध TOR का इस्तेमाल कर रहा हो, तो IPDR की जांच करके हम कैसे इस बात की पुष्टि कर सकते हैं?  
 (1) स्रोत पोर्ट का विश्लेषण करके  
 (2) डेस्टिनेशन पोर्ट का विश्लेषण करके  
 (3) सार्वजनिक आइ पी का विश्लेषण करके  
 (4) उपरोक्त सभी
125. आइ.पी.डी.आर. शब्द का अर्थ है –  
 (1) Intellectual Property Detail Record  
 (2) International Public Domain Record  
 (3) Internet Protocol Detail Record  
 (4) उपरोक्त में से कोई नहीं
126. जेल में इस्तेमाल होने वाले फोन का सबसे अच्छा संकेतक है –  
 (1) सी.डी.आर. में एकाधिक आई.एम.ई.आई और कई सैल आइ डी  
 (2) सी.डी.आर. में कई सैल आइ डी और बहुत आई एम एस आई  
 (3) उपरोक्त (1) व (2)  
 (4) उपरोक्त में से कोई भी नहीं
127. आई.एम.ई.आई. के प्रथम 6 – 8 अंक दर्शाते हैं –  
 (1) टी.ए.सी.  
 (2) एम.ए.सी.  
 (3) आई.पी.एम.ए.सी.  
 (4) आई.पी.वी<sub>6</sub> एम.ए.सी.
128. जीरो डे अटैक होता है –  
 (1) जिस दिन एप्लिकेशन या OS जारी किया जाता है  
 (2) पैच उपलब्ध होने से पहले  
 (3) विक्रेता को भेद्यता पता होने से पहले  
 (4) उपरोक्त (2) व (3)

129. Which of the following is not correct?
- (1) Web cache does not has its own disk space
  - (2) Web cache can act both like server and client
  - (3) Web cache reduces the response time
  - (4) Web cache contains copies of recently requested objects
130. The e-mail header provides information about –
- (1) Senders IP address
  - (2) Recipient IP address
  - (3) Both (1) and (2)
  - (4) None of these
131. The best way of browsing internet anonymously without registering for any service –
- (1) Using Safari
  - (2) Using TOR
  - (3) Both (1) & (2)
  - (4) None of the above
132. Bitcoin was created by –
- (1) John Mcafee
  - (2) Sir William Herschel
  - (3) Satoshi Nakamoto
  - (4) Mitsuru Ebihara
133. The P2P stands for –
- (1) Password to password
  - (2) Peer to Peer
  - (3) Product to product
  - (4) Private Key to Public Key
134. The Artificial Intelligence was invented by –
- (1) Fisher Ada
  - (2) Alan Turing
  - (3) John Mc Carthy
  - (4) Allen New Well
135. What is the term for when a block chain splits?
- (1) A Fork
  - (2) A Merger
  - (3) A Division
  - (4) None of the above
129. निम्नलिखित में से कौन सही नहीं है?
- (1) वेब कैशे का अपना डिस्क स्पेस नहीं है।
  - (2) वेब कैशे सर्वर व क्लाइंट दोनों की तरह कार्य करता है
  - (3) वेब कैशे का प्रतिक्रिया समय को घटाना
  - (4) वेब कैशे हाल ही में अनुरोधित वस्तुओं को संधारित रखता है।
130. ई-मेल हैडर किस बारे में जानकारी देता है –
- (1) भेजने वाले का आई पी एड्रेस
  - (2) प्राप्तकर्ता का आई पी एड्रेस
  - (3) उपरोक्त (1) व (2)
  - (4) इनमें से कोई नहीं
131. किसी भी सेवा के लिए पंजीकरण किए बिना गुमनाम रूप से इंटरनेट ब्राउज़ करने का सबसे अच्छा तरीका –
- (1) सफारी का उपयोग करके
  - (2) टी ओ आर का उपयोग करके
  - (3) उपरोक्त (1) व (2)
  - (4) उपरोक्त में से कोई भी नहीं
132. बिटकॉइन किसने बनाया?
- (1) जॉन मैकफे
  - (2) सर विलियम हर्शल
  - (3) सातोशी नाकामोटो
  - (4) मीतसुरू एबीहारा
133. P2P का मतलब है –
- (1) पासवर्ड टू पासवर्ड
  - (2) पीयर टू पीयर
  - (3) प्रोडक्ट टू प्रोडक्ट
  - (4) प्राइवेट की टू पब्लिक की
134. आर्टिफिशियल इंटेलिजेंस का आविष्कार किसने किया –
- (1) फिशर अदा
  - (2) एलन ट्यूरिंग
  - (3) जॉन मैकार्थी
  - (4) एलन न्यूवेल
135. जब एक ब्लॉक चेन विभाजित होता है, तो उसके लिए क्या शब्द है?
- (1) एक फोर्क
  - (2) एक मर्जर
  - (3) एक डिविजन
  - (4) उपरोक्त में से कोई नहीं

136. What is the Arduino UNO?  
 (1) Software  
 (2) Hardware  
 (3) Network  
 (4) Protocol
137. The MQTT abbreviation stands for –  
 (1) Major Queue Telemetry Transport  
 (2) Minor Queue Telemetry Transport  
 (3) Message Queue Telemetry Transport  
 (4) None of the above
138. Which of the following is not an anonymous search engine?  
 (1) start page  
 (2) baidu  
 (3) searx.me  
 (4) qwant
139. The formal name of the drone is –  
 (1) UAP  
 (2) QUA  
 (3) PAV  
 (4) UAV
140. The magnetic strip of the credit card contains –  
 (1) One track  
 (2) Two tracks  
 (3) Three tracks  
 (4) Five tracks
141. The United Nations Commission on International Trade Law (UNCITRAL) adopted model law on electronic commerce in –  
 (1) 1996  
 (2) 1997  
 (3) 1991  
 (4) 1995
142. Under which section of IT Act the Indian Computer Emergency Response Team was established?  
 (1) 79A  
 (2) 70B  
 (3) 61  
 (4) None of the above
143. The significance of HASH function is –  
 (1) To ensure the integrity of the evidence  
 (2) To establish authenticity  
 (3) To verify evidence  
 (4) All the above
136. Arduino UNO क्या है?  
 (1) सॉफ्टवेयर  
 (2) हार्डवेयर  
 (3) नेटवर्क  
 (4) प्रोटोकॉल
137. एम.क्यू.टी.टी. का क्या अभिप्राय है?  
 (1) Major Queue Telemetry Transport  
 (2) Minor Queue Telemetry Transport  
 (3) Message Queue Telemetry Transport  
 (4) उपरोक्त में से कोई भी नहीं
138. निम्नलिखित में से कौन एक अनोनिमस खोज इंजन नहीं है?  
 (1) स्टार्ट पेज  
 (2) बायडू  
 (3) searx.me  
 (4) क्वांट
139. ड्रोन का औपचारिक नाम है –  
 (1) यू ए पी  
 (2) क्यू यू ए  
 (3) पी ए वी  
 (4) यू ए वी
140. क्रेडिट कार्ड की चुंबकीय पट्टी में शामिल होते हैं—  
 (1) एक ट्रेक  
 (2) दो ट्रेक  
 (3) तीन ट्रेक  
 (4) पाँच ट्रेक
141. अंतर्राष्ट्रीय व्यापार कानून पर संयुक्त राष्ट्र आयोग (UNCITRAL) ने इलेक्ट्रॉनिक कॉमर्स पर मॉडल कानून कब अपनाया?  
 (1) 1996  
 (2) 1997  
 (3) 1991  
 (4) 1995
142. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम आई टी एक्ट के किस धारा के अन्तर्गत स्थापित की गई?  
 (1) 79A  
 (2) 70B  
 (3) 61  
 (4) उपरोक्त में से कोई नहीं
143. हैश फंक्शन का महत्त्व है –  
 (1) सबूत की अखंडता सुनिश्चिता करना  
 (2) प्रमाणिकता स्थापित करना  
 (3) सबूत सत्यापित करना  
 (4) उपरोक्त सभी

144. The chain of custody begins at –
- (1) Scene of crime
  - (2) The laboratory
  - (3) Malkhana
  - (4) Prison
145. A DoS attack coming from a large number of IP addresses, making it hard to manually filter or crash the traffic from such sources is known as –
- (1) GoS attack
  - (2) DDoS attack
  - (3) EDoS attack
  - (4) PDoS attack
146. What is the attack called “Evil Twin”?
- (1) MAC Spoofing
  - (2) Session Hijacking
  - (3) Rogue Access Point
  - (4) ARP Poisoning
147. The Public Key is defined as –
- (1) A Key pair used to create digital signature
  - (2) A Key pair used to verify digital signature
  - (3) Both (1) and (2)
  - (4) None of the above
148. Staxnet is a –
- (1) Virus
  - (2) Worm
  - (3) Trojan
  - (4) None of the above
149. The usage of antistatic band is recommended to –
- (1) Nullify the effect of Electromagnetic radiations
  - (2) Nullify the static current
  - (3) Both (1) and (2)
  - (4) None of the above
150. The section 65 B of IEA, 1872 deals with –
- (1) Admissibility of Electronic record
  - (2) Admissibility of Elementary record
  - (3) Admissibility of Expert report
  - (4) None of the above
144. चेन ऑफ कस्टडी कहाँ से शुरू होती है –
- (1) अपराध घटना स्थल
  - (2) प्रयोगशाला में
  - (3) मालखाना
  - (4) जेल
145. बड़ी संख्या में IP ऐड्रेस से आने वाले DoS अटैक, ऐसे स्रोतों से ट्राफिक को मैनुअल रूप से फिल्टर करना या क्रैश करना कठिन बना देता है, एक रूप में जाना जाता है –
- (1) GoS अटैक
  - (2) DDoS अटैक
  - (3) EDoS अटैक
  - (4) PDoS अटैक
146. “ईविल ट्विन” अटैक को कहाँ जाता है?
- (1) मैक स्फूफिंग
  - (2) सेशन हाईजैकिंग
  - (3) रोग एक्सेस प्वाइंट
  - (4) ए आर पी पोइजनिंग
147. पब्लिक की को परिभाषित करता है –
- (1) डिजिटल हस्ताक्षर बनाने के लिये उपयोग में लाई जाने वाली प्रमुख जोड़ी
  - (2) डिजिटल हस्ताक्षर को सत्यापित करने के लिये उपयोग की जाने वाली प्रमुख जोड़ी
  - (3) उपरोक्त (1) व (2)
  - (4) उपरोक्त में से कोई भी नहीं
148. स्टैक्सनेट एक –
- (1) वायरस है
  - (2) वर्म है
  - (3) ट्रोजन है
  - (4) उपरोक्त में से कोई भी नहीं
149. एंटीस्टैटिक बैंड के इस्तेमाल की सलाह दी जाती है –
- (1) विद्युत चुम्बकीय प्रभाव को खत्म करने के लिये
  - (2) स्टैटिक करंट को शून्य करने के लिये
  - (3) उपरोक्त (1) व (2)
  - (4) उपरोक्त में से कोई भी नहीं
150. भारतीय साक्ष्य अधिनियम, 1872 की धारा 65B संबंधित है—
- (1) इलेक्ट्रॉनिक रिकॉर्ड की स्वीकार्यता
  - (2) प्राथमिक रिकॉर्ड की स्वीकार्यता
  - (3) विशेषज्ञ रिपोर्ट की स्वीकार्यता
  - (4) उपरोक्त में से कोई भी नहीं

Space for Rough Work / रफ कार्य के लिए जगह