

Section 1 - Group One

1) Applications of IoT include

- A) Logistics
 - B) Retails
 - C) All the above options
 - D) Smart cities
-

2) Mention the method that analyzes each encrypted, compressed and password protected files in acquiring evidences

- A) Analysis of e-mail messages
 - B) File Analysis
 - C) Log File Analysis
 - D) Data hiding Analysis
-

3) Which type of crime analysis furnishes information concerning long-range crime related problems?

- A) All of these
 - B) Tactical crime analysis
 - C) Strategic Crime Analysis
 - D) Administrative crime analysis
-

4) Who use Hacking to take forward their other criminal activities and have little interest in fame?

- A) Old guards
- B) Virus writer
- C) Novice hacker
- D) Petty Thieves

5) Choose the Sub-Section of 66, that covers crimes related to Privacy Violations

- A) 66F
 - B) 66E
 - C) 66D
 - D) None of the above options
-

6) Point out the attack type where the attacker changes the IP address after gaining control of a trusted client and communicates with the server.

- A) Replay attack
 - B) Session hijacking
 - C) MitM attack
 - D) IP spoofing
-

7) What are the ethics to be followed in Cyberspace to be a good Citizen?

- A) Adhere to copyright restrictions
 - B) Avoid impersonating another person
 - C) All of the above options
 - D) Avoid engaging in inappropriate conduct
-

8) Social media tips and practices involve

- A) A and C
- B) Creating social media policy
- C) Limiting social media access
- D) Not Performing Ethical operations

9) Applications that create queries dynamically can be considered as a risk source of

- A) Active attacks
 - B) Injection Attacks
 - C) Passive attacks
 - D) Forgery
-

10) Analyze critically and Check the validity of the following statements:

1.SSL is used to provide access to databases securely with the help of public key and secret key technology

2.Biometrics cannot be guessed or compromised easily

- A) FT
 - B) TF
 - C) TT
 - D) FF
-

11) Select from the following methods that specifies the study of a person through his writing style

- A) Signature Analysis
 - B) Stylometry
 - C) Crime Analysis
 - D) Modus Operandi
-

12) The issues like accepted standards and fit-to-practice can be classified under this category in Digital Forensics

- A) Administrative Issues
- B) Ethical Issues
- C) Legal Issues
- D) Technical Issues

13) Digital Signatures make use of this type of Cryptography

- A) Private Key
 - B) Digital Certificates
 - C) Digital key
 - D) Public key
-

14) Point out the most widely used open source Digital Forensic Tool

- A) Autopsy
 - B) Wireshark
 - C) FTK
 - D) CAINE
-

15) Pick up the Authentication type that uses QR validation code

- A) Multi-factor authentication
 - B) API authentication
 - C) Mobile Authentication
 - D) Continuous authentication
-

16) How the security and flexibility of the National infrastructure and services can be improved? It can be achieved through

- A) Cyber defense Centre
- B) National Cyber Security Strategy
- C) National Security Centre
- D) Cyber investigation service Centre

17) Choose the method that engages the process of using automated testing tools like network security scanners

- A) Vulnerability Analysis
 - B) Intrusion Prevention System
 - C) Intrusion Detection System
 - D) Intrusion Detection and Prevention System
-

18) Assess the validity of the Statements:

- 1.Port scanners use unique gadgets to spy the traffic between computers inside the network.
2. In passive attack, the attacker communicates data to all divisions or blocks during data transmission.

- A) FT
 - B) TF
 - C) TT
 - D) FF
-

19) Which step in CPS workflow tracks the physical system and its environment?

- A) Actuation
 - B) Monitoring
 - C) Networking
 - D) Computing
-

20) What causes the loss of CIA triad in mobile devices?

- A) Multiple user logging
- B) Coding issues
- C) Bluetooth attacks
- D) Mobile browsing

21) Name the Authentication Method that authenticates a person based on the physical or behavioural characteristics.

- A) Biometric based authentication
 - B) Object-based authentication
 - C) None of these
 - D) Knowledge based authentication
-

22) This is the first major known Cyber-Attack

- A) Botnets
 - B) Morris Worm
 - C) Virus
 - D) Macro virus
-

23) One of the main functions of maintaining integrity in mail server can be done through

- A) Backing up of data
 - B) Protection
 - C) Testing
 - D) Confidentiality
-

24) Simultaneous actions by the operators in different dimensionalities indicate this feature of Cyberspace

- A) Effectiveness
- B) Space
- C) Efficiency
- D) Interactive

25) Security compromise in a network occurs mainly due to this

- A) Intrusions
 - B) Internet Connections
 - C) Wireless Connection
 - D) Unauthorized Access
-

26) Mention the mobile data security strategies the employees should use

- A) Protecting data on lost and stolen devices
 - B) All the above options
 - C) Application security
 - D) Secure Web browsing habits
-

27) Guess the primary motives behind Cyber-attacks

- A) Non-Religious
 - B) Both B and C
 - C) Entertainment Purpose
 - D) Financial Gain
-

28) Authenticating or Authorizing valid users are the fundamental techniques used in

- A) Both A and B
- B) Information Security
- C) Network Security
- D) Application Security

29) Select the safest form of earning Virtual Currencies

- A) Offer based Method
 - B) Both A and B
 - C) Pay for Virtual Currency Method
 - D) Self-effort based method
-

30) The Difficulty in identifying the user or a location in Cyberspace indicates this

- A) Asynchronous
 - B) Asymmetry
 - C) Anonymity
 - D) Abstract
-

31) Which of the following is a risk management strategy?

- A) All of the above
 - B) Consider stakeholder's perception
 - C) Apply suitable policies and related controls
 - D) Risk capacity and need determination
-

32) When was the first Cyber Offence conducted and recorded?

- A) 1820
- B) 1859
- C) 1890
- D) 1867

33) Authentication approaches depend upon what the user

- A) All the above three options
 - B) Is
 - C) Has
 - D) Knows
-

34) Choose the appropriate option after analyzing the following statements:

1. In a public Blockchain anyone can read, run and transact

2. Private Blockchain is low efficient

- A) TT
 - B) TF
 - C) FT
 - D) FF
-

35) Pick up the first application of Blockchain Technology

- A) Bitcoin
 - B) Virtual Currency
 - C) Public Blockchain
 - D) Crypto Currency
-

36) List the elements of Incident Analysis in Computer Security

- A) Create a Log Retention Policy
- B) Keeping the Host Clocks Synchronized
- C) All the above options
- D) Profile Networks

37) Select the Authentication methods from the following that can be easily cracked

- A) PINs
 - B) Password or Knowledge based
 - C) Biometric authentication
 - D) Both A and C
-

38) This Profiling Method helps the Investigation Officers to judge a person's moral values and attitudes

- A) Criminal Profiling
 - B) Digital Forensics
 - C) Psychological Profiling
 - D) Stylometric Analysis
-

39) Indicate the term that is used to denote the set of rules and arrangements to carry out Blockchain operations

- A) Consensus
 - B) Block
 - C) Chain
 - D) Miners
-

40) List the branches of Artificial Intelligence used in IDS.

- A) Genetic Algorithm, Clustering
- B) Fuzzy logic, Data Mining
- C) Both A and B
- D) None of the above

41) Which Forensics uses Audio Visual Footages for Analysis?

- A) Memory Forensics
 - B) Digital Forensics
 - C) Mobile Device Forensics
 - D) Digital Video/Audio Forensics
-

42) Identify the type of attacks that consume network bandwidth and flood the networks with data

- A) Organized attacks
 - B) Protocol attacks
 - C) Application attacks
 - D) Volume based attacks
-

43) Fix the stage of the BEA framework where the Investigators collect characteristics of the Crime Scene

- A) Victimology
 - B) Equivalent Forensic Analysis
 - C) Criminal Characteristics
 - D) Assessment of Crime Scene
-

44) Which structure outlines the essential needs to support and implement the security policy?

- A) Biba model
- B) Security Model
- C) ISO 27001 model
- D) Access control

45) The conduct of fraudulent activity is the characteristic of

- A) Spoofing
 - B) Accessibility
 - C) Criminality
 - D) Authority
-

46) The actual relationships between the elements of the network are abstracted in this layer

- A) Logical Network
 - B) Cloud
 - C) Physical Network
 - D) Cyberspace
-

47) Mention the name of Cyber Crime that is executed through email, social media, chat rooms, instant messaging

- A) Piracy
 - B) Cyber-proofing
 - C) Cyber Stalking
 - D) Data exploitation
-

48) Identify the process that is systematic and analytical in nature to provide timely and appropriate information related to crime.

- A) Authentication
- B) Crime Analysis
- C) Digital Forensics
- D) Cyber Security

49) Choose the common security risk in Social Media

- A) Common social media accounts
 - B) Human Error
 - C) Vacation Robbery
 - D) Buying illegal things
-

50) Name the process that identifies the path to transfer data over the network

- A) Routing
- B) Packet filtering attack
- C) DoS attack
- D) Persistent attack

Section 2 - Group Two

51) List the shortcomings of Cyberspace

- A) Slow performance
 - B) Complexity
 - C) Medium of connectivity for Data Theft
 - D) Platform for Criminal activities
-

52) The issues faced during IoT device manufacturing are

- A) Improper device function
 - B) System slow down
 - C) Cost
 - D) Weak security solutions
-

53) E-mail hacking, Defamation and Phishing are the Cybercrimes against

- A) Assets
 - B) Nation
 - C) Organizations
 - D) Individuals
-

54) Choose the various formats of electronic documents available

- A) Metadata
- B) Excel spreadsheet
- C) Power point
- D) Voice mail

55) Identify the constraints to be monitored in a phished e-mail

- A) Fake rewards
 - B) Suspicious or irrelevant e-mail
 - C) Fake addresses
 - D) Clone of existing e-mail
-

56) The offences which are recognized by both Indian Penal Code and Information Technology Act 2000 are

- A) E-mail spoofing
 - B) Bogus websites
 - C) Phishing
 - D) Theft of Internet time
-

57) How to prevent the compromise of broken authentication and session management?

- A) Cookies
 - B) Session Keys
 - C) Session tokens
 - D) Addresses
-

58) Examples for non-malicious attack

- A) Accidental erasing of data
- B) Tracking cookies
- C) Registry corruption
- D) Sasser attack

59) Mention the details WHOIS database contains

- A) Internet Address
 - B) Domain Name
 - C) Contact number
 - D) System details
-

60) What are the characteristics to be considered in the construction of a behavioural profile?

- A) Data collection
 - B) Victim analysis
 - C) Information sources
 - D) Crime scene
-

61) Identify the attacks on Service Layer of SOA

- A) Black hole Attack
 - B) Cross-Site Scripting
 - C) Cryptography Injection
 - D) Wormhole Attack
-

62) Guess the areas that focus on recent Criminal Profiling research

- A) Overall differentiation
- B) Behavioural inconsistency
- C) Individual differentiation
- D) Behavioural consistency

63) Highlight the functions of Analysis of Crime

- A) Provision of Investigative Leads
 - B) Forecasting future crimes
 - C) Identification of crime patterns
 - D) Assistance in Case clearance process
-

64) Identify the suitable Countermeasures to a TCP SYN flood attack

- A) Firewalls can be installed to suspicious traffic
 - B) Increasing open time connection, when not used
 - C) Connection queue size should be decreased
 - D) Reducing open time connection, when not used
-

65) What are the special features of Anomaly-based Detection System?

- A) Track new threats
 - B) Perform vulnerability testing
 - C) Discard vulnerabilities
 - D) Detect new attacks
-

66) Choose the approaches used for Criminal Profiling

- A) Deductive Profiling
- B) Computer forensic tools
- C) Inductive Profiling
- D) E-forensic tools

67) Produce the Criteria for selecting a Forensic Firm

- A) Knowledge in Data Recovery
 - B) Straight Forward Aspect
 - C) Knows the guidelines of the Firm
 - D) Technical Expertise
-

68) Select the appropriate methods used to obtain and generate Virtual Currency

- A) Self-effort based
 - B) Offer-based
 - C) Exchange of Virtual Currency
 - D) Loyalty-based
-

69) Point out the Ethical issues in Computing

- A) Private organizations
 - B) Access rights
 - C) Firewalls
 - D) Personal privacy
-

70) Choose the important Process models used for Computer Forensics Investigation

- A) Seizure Model
- B) Extended Model for Cyber Crime Investigation
- C) Framework for Digital Investigations
- D) Statistical Model

71) Hackers make use of cookies to

- A) Access the system
 - B) Log key strokes
 - C) Block threats
 - D) Capture screenshots
-

72) Highlight the advantages of Cloud Forensics

- A) Data Abundance
 - B) Forensics-as-a-service
 - C) Lack of Policies
 - D) Higher Security
-

73) Indicate the functions of Indian Computer Emergency Response Team

- A) Block cyber threats
 - B) Correlates events
 - C) Predicting cybersecurity incident occurrence
 - D) Issuing guidelines
-

74) What are the rules included in Take-Grant protection security model?

- A) Take
- B) Create
- C) Manage
- D) Grant

75) Evidences can be collected from the digital devices like

- A) Written Document
 - B) Mobile Devices
 - C) SMS
 - D) Web cameras
-

76) Select the Cloud Security Risks from the following

- A) Diminished Customer Trust
 - B) Theft of Intellectual Property
 - C) Decreased Customer Chun
 - D) Service type
-

77) Based on the provisions of IPC Act, RBI classified frauds and offences as

- A) Cash shortages
 - B) Gratification
 - C) Criminal breach of trust
 - D) Unauthenticated credit facilities
-

78) Choose the threats faced by Security Auditors during the audit process

- A) Malicious insiders
- B) Natural disasters
- C) Negligent employees
- D) Unknown entities

79) Which of the following functions of Information Systems are improved by Data Integrity?

- A) Reusability
 - B) Readability of Sensitive Information
 - C) Performance
 - D) Stability
-

80) The existence of Cyber law is due to the increase in

- A) Crimes committed over Internet
 - B) Usage of Computer resources
 - C) Usage of Cyberspace
 - D) Need of the hour
-

81) The characteristics of type D Computer Security Classification

- A) Lowest level
 - B) Minimum protection
 - C) High protection
 - D) Individual Access
-

82) Identify the elements the investigator has to examine during Examination and Analysis Phase

- A) Partitions
- B) Network
- C) Operating system
- D) File System

83) Pick out the important features of Crime Analysis

- A) Protocols
 - B) Signature
 - C) Social Network Analysis
 - D) Personality of the Criminal
-

84) Mention the factors to be considered during Threat Assessment

- A) Regulation and Compliance
 - B) History of the Organization
 - C) On-going Business trends
 - D) Current Cyber Security Trends
-

85) Route Attack, Authentication Attack and Tampering with the Network are the Threat types in this layer of CPS

- A) Control Process
 - B) Communication
 - C) Transport
 - D) Physical Component
-

86) List the three main conducts used for IRC crimes

- A) Twin Attack
- B) Vocal Attack
- C) DDoS Attack
- D) Torrent Attack

87) List the IoT Forensic Challenges

- A) Identifying the Device Type
 - B) Location of Data
 - C) Data Format Preservation
 - D) Finding Google Accounts
-

88) Select the legal issues in Cyberspace

- A) Spam
 - B) Spying
 - C) Scam
 - D) Domain Name issue
-

89) Select the primary authentication factors from the list

- A) Location factor
 - B) Possession factor
 - C) Inherence factor
 - D) Knowledge factor
-

90) Choose the protection methods used against unauthorized administrators

- A) Configure for DoS attacks
- B) Block system
- C) Run network monitor tools to sniff packets
- D) Permit access

91) The primary components of E-mail System are

- A) Network
 - B) Protocols
 - C) Mail Clients
 - D) Mail Servers
-

92) Collect the Stylometry Features from the following

- A) Syntactic Feature
 - B) Idiosyncratic Feature
 - C) Biometric Feature
 - D) Lexical Feature
-

93) What do the Ethical Hackers do?

- A) Steal data
 - B) Perform Penetration Testing
 - C) Conduct Vulnerability Assessment
 - D) Fix Security loopholes
-

94) Trace the sources from which the evidence can be captured easily and effectively

- A) Portable devices
- B) Backup media
- C) Network sharing
- D) E-mail server

95) The quality of enrolled biometric sample is affected by

- A) Improper actions
 - B) Environmental conditions
 - C) Accidental actions
 - D) Deliberate events
-

96) Point out the suitable applications of Face recognition system

- A) Employee sign-in
 - B) On-line Shopping
 - C) Mobile Phones
 - D) Customer account login
-

97) Summarize the issues faced by the Digital Forensics experts during examination

- A) Administrative issues
 - B) Coding issues
 - C) Legal issues
 - D) Technical issues
-

98) The Detectives of Cyber Crime make use of forensic tools for these operation

- A) Accumulate
- B) Frame
- C) Index
- D) Merge

99) The ways in which Mobile Devices can be protected

- A) Do not back up information
 - B) Protect using passwords
 - C) Keep Bluetooth on
 - D) Update firewall and anti-virus software patches
-

100) Extract some form of Internet communication vulnerabilities from the following

- A) Protocol-based vulnerabilities
- B) Invalid user inputs
- C) Unchecked user inputs
- D) System-based risks

Answer Key**Question Paper No: 60873_6****Section 1 - Group One**

1	C	26	B
2	D	27	B
3	C	28	A
4	D	29	A
5	B	30	C
6	B	31	A
7	C	32	A
8	A	33	A
9	B	34	B
10	A	35	A
11	B	36	C
12	A	37	B
13	D	38	C
14	B	39	A
15	C	40	C
16	B	41	D
17	A	42	D
18	D	43	D
19	B	44	B
20	A	45	C
21	A	46	A
22	B	47	C
23	A	48	B
24	C	49	B
25	A	50	A

Section 2 - Group Two

51	B,D	76	A,B
52	A,C,D	77	A,C
53	A,B	78	B,C,D
54	A,B,C,D	79	A,B,C
55	A,B,D	80	B,C,D
56	A,,D	81	C,D
57	A,B,C	82	B,C,D
58	A,B,	83	A,B
59	A,C,D	84	A,C,D
60	B,C,D	85	B,D
61	A,C	86	B,C,D
62	A,,D	87	A,B,C
63	A,B,C,D	88	A,B
64	B,C	89	B,C,D
65	A,C	90	B,D
66	B,D	91	B,C
67	A,C	92	A,C,D
68	A,B,C	93	A,C,D
69	A,,D	94	A,B,C,D
70	C,D	95	A,C,D
71	B,C	96	A,B,C
72	A,,D	97	A,C,D
73	C,D	98	B,D
74	A,B,C	99	C,D
75	B,D	100	B,D