5500+
Objective Solved Questions

Volume-10
Network Security
Basics of Communication
Web Development

ENGINEERS ACADEMY®
Your GATEway to Professional Excellence
IES • GATE • PSUs • JTO • IAS • NET

RSSB

RAJASTHAN STAFF SELECTION BOARD

SENIOR COMPUTER INSTRUCTOR

Subjectwise, Chapterwise Objective Solved Questions

Key Features

- **Topic-wise Bifurcation of Questions**
- Most of the Questions having Either Solution or Explanations.
- **Also Useful for IA, NIC, BCI & other Computer Exams**

E info@engineersacademy.org W www.engineersacademy.org
National Board Helpline Number : + 91 809 444 1777

Publisher and Distributor

Engineers Academy Publications

100-102, Ram Nagar, Bambala Puliya, Toll Tax,
Tonk Road, Pratap Nagar, Jaipur (Rajasthan)-302033
E-Mail : engineers.academy.india@gmail.com

ISBN : 978-93-93531-78-0

First Edition	:	**2023**
Second Edition	:	**2026**

Price : ₹ 150.00

DIRECTOR'S *Message*

To reach heights one must start climbing and if the journey is difficult then perseverance is the key to success. As a teacher we have realized over past years that success in any competitive exam requires hard work and proper guidance. **Engineers Academy** with its unique teaching methodologies has always proved that we meet the expectations of thousands of students and parents to make their dreams come true. With changing patterns, we have adapted ourselves to deliver the best and ensure better results.

This book has been organized and executed with a lot of care, dedication and passion for lucidity. A conscious attempt has been made to simplify the concepts to facilitate better understanding of the subject.

Engineers Academy has many successful stories of students who secured All India Rank in ESE, GATE, PSUs and JEn. Now we invite you to become a part of Engineers Academy to explore and achieve ultimate goal of your life. We promise to provide you quality guidance with competitive environment which is far advanced and ahead than the reach of other institution.

We would feel satisfied if the book meets the needs of the students for whom it is meant.

Lastly, we are thankful to all the engineers, authors whose work has been the source of enlightenment, inspiration and guidance in presenting this book.

It is hoped that the book in its new form will enjoy its ever increasing popularity.

Regards

Dr. Pankaj Goyal

Preface

This book has been written to meet the growing requirements of candidates appearing for Senior Computer Instructor and other competitive Examinations. Though every candidate has ability to succeed but competitive environment, in-depth knowledge, quality guidance, time management and good source of study is required to achieve goals.

This book includes Multiple Choice Questions (MCQ's) which works as a mock exam practice for the reader. Questions of all the subject have been organized in systematic, concepts oriented and error less manner so that it become easy and interesting for even a beginner to understand. It is a very convenient book and must be solved by candidate aiming for competitive exams.

After solving this booklet students can feel encouraged and develop confidence to attempt each and every type of numerical as well as theoretical problems. Each problems explains solving approach so that at the end, so the reader is well equipped to be able to apply any type of problem solving requirement and distinctly choose one strategy or type from the other.

We hope this book will be proved an important tool to succeed in Basic and Senior Computer Instructor and other competitive Examinations.

Even though, enough readings were given for correcting the error and printing mistakes, due to human tendency there could be some minor typos in the book. If any such typos found, they will be highly appreciated and in corporated in the next edition. Also, please provide your valuable suggestions at :engineers.academy.india@gmail.com

Wish you all the best. Have a nice reading.

Team of
Engineers Academy Publications

Contents

Volume 10

1 Network Security

OBJECTIVE QUESTION

1. In the digital signature technique when the whole message is signed using an asymmetric key, the receiver of the message uses _____ to verify the signature.

(a) Her or his own public key

(b) Her or his own private key

(c) The sender's public key

(d) None of the choices are correct.

2. What is the ethics behind training how to hack a system?

(a) To think like hackers and know how to defend such attacks

(b) To hack a system without the permission

(c) To hack a network that is vulnerable

(d) To corrupt software or service using malware

3. The legal risks of ethical hacking include lawsuits due to _____ of personal data.

(a) Stealing (b) Disclosure

(c) Deleting (d) Hacking

4. After performing _____ the ethical hacker should never disclose client information to other parties.

(a) Hacking

(b) Cracking

(c) Penetration testing

(d) Exploiting

5. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

(a) Malware (b) Spyware

(c) Adware (d) All of the above

6. Which one of the following is a type of antivirus program?

(a) Quick heal (b) Mcafee

(c) Kaspersky (d) All of the above

7. Which one of the following refers to the technique used for verifying the integrity of the message?

(a) Digital signature (b) Decryption algorithm

(c) Protocol (d) Message Digest

8. Which of the following port and IP address scanner famous among the users?

(a) Cain and Abel (b) Angry IP Scanner

(c) Snort (d) Ettercap

9. Which of the following is not a type of scanning?

(a) Xmas Tree Scan (b) Cloud scan

(c) Null Scan (d) SYN Stealth

10. Code Red is a type of _____

(a) An Antivirus Program

(b) A photo editing software

(c) A computer virus

(d) A video editing software

11. What is the full form of LDAP?

(a) Light Weight Directory Access Provider

(b) Light Weight Directory Access Protocol

(c) Light Weight Directory Access Program

(d) Light Weight Directory Access Protection

12. What is called a single point of access for several networking services?

(a) Phishing (b) Web service

(c) Directory service (d) Worms

13. The type of encoding in which manipulation of bit streams without regard to what the bits mean is .....

(a) Destination encoding

(b) Entropy encoding

(c) Source encoding

(d) Differential encoding

14. The protocol used to provide security to e-mails?

(a) POP (b) PGP

(c) SNMP (d) HTTP

15. The length of the key in one time pad method is .....

(a) Random (b) Fixed

(c) 64 (d) 56

16. The text that gets transformed using algorithm cipher is called?

(a) Complex text (b) Transformed text

(c) Plain text (d) Scalar text

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

(a) Authentication (b) Identification

(c) Validation (d) Verification

18. Which of these is a part of network identification?
(a) UserID (b) Password
(c) OTP (d) Fingerprint

19. The information that gets transformed in encryption is _____
(a) Plain text (b) Parallel text
(c) Encrypted text (d) Decrypted text

20. A _____ is a trusted third party that solves the problem of symmetric-key distribution.
(a) CA (b) KDC
(c) TLS (d) Firewall

21. In the _____ mode, the IPSec header is added between the IP header and the rest of the packet.
(a) Transport
(b) Tunnel
(c) Transition
(d) None of the choices are correct.

22. The information that gets transformed in encryption is _____
(a) Plain text (b) Parallel text
(c) Encrypted text (d) Decrypted text

23. An algorithm in encryption is called _____.
(a) Algorithm (b) Procedure
(c) Cipher (d) Module

24. Network security consists of:
(a) Protection (b) Detection
(c) Reaction (d) All of the above

25. Interaction between the client and server starts via the _____ message.
(a) client_hi (b) client_hello
(c) server_hello (d) server_hi

26. What is true about Email security in Network security methods?
(a) Phishing is one of the most common ways attackers gain access to a network.
(b) You should know what normal network behavior looks like so that you can spot anomalies or breaches as they happen.
(c) You need to employ hardware, software, and security processes to lock those apps down.
(d) All of the above

27. The text that gets transformed using algorithm cipher is called?
(a) Complex text (b) Transformed text
(c) Plain text (d) Scalar text

28. Which of these is a part of network identification?
(a) UserID (b) Password
(c) OTP (d) Fingerprint

29. You are working on a router that has established privilege levels that restrict access to certain functions. You discover that you are not able to execute the commandshow running-configuration. How can you view and confirm the access lists that have been applied to the Ethernet 0 interface on your router?
(a) Show access-lists
(b) Show interface Ethernet 0
(c) Show ip access-lists
(d) Show ip interface Ethernet 0

30. What router command allows you to determine whether an IP access list is enabled on a particular interface?
(a) Show ip port
(b) Show access-lists
(c) Show ip interface
(d) Show access-lists interface

31. WTLS stands for?
(a) Wireless Transport Security Layer
(b) Wireless Transfer System Layer
(c) Wireless Transfer Security Layer
(d) Wireless Transport System Layer

32. A small program that changes the way a computer operates.
(a) Worm (b) Trojan
(c) Bomb (d) Virus

33. An indirect form of surveillance.
(a) Honey pot (b) Logical
(c) Security (d) Intrusion

34. An attack in which the user receives unwanted amount of e-mails.
(a) Smurfing (b) Denial of service
(c) E-mail bombing (d) Ping storm

35. What is the standard IANA port number used for requesting web pages?
(a) 80 (b) 53
(c) 21 (d) 25

36. Which of the following process is used for verifying the identity of a user?
(a) Authentication (b) Identification
(c) Validation (d) Verification

37. Which of the following modes of operation in DES is used for operating?
(a) Cipher Feedback Mode (CFB)
(b) Cipher Block chaining (CBC)
(c) Electronic code book (ECB)
(d) Output Feedback Modes (OFB)

38. Using Rivest, Shamir, Adleman cryptosystem with p=7 and q=9. Encrypt M=24 to find ciphertext. The Ciphertext is:
(a) 42 (b) 93
(c) 114 (d) 103

39. In TCP, sending and receiving data is done as _____
(a) Stream of bytes
(b) Sequence of characters
(c) Lines of data
(d) Packets

40. To achieve reliable transport in TCP, _____ is used to check the safe and sound arrival of data.
(a) Packet (b) Buffer
(c) Segment (d) Acknowledgment

41. The value of acknowledgement field in a segment defines _____
(a) Sequence number of the byte received previously
(b) Total number of bytes to receive
(c) Sequence number of the next byte to be received
(d) Sequence of zeros and ones

42. What is the ethics behind training how to hack a system?
(a) To think like hackers and know how to defend such attacks
(b) To hack a system without the permission
(c) To hack a network that is vulnerable
(d) To corrupt software or service using malware

43. Performing a shoulder surfing in order to check other's password is _____ ethical practice.
(a) A good
(b) Not so good
(c) Very good social engineering practice
(d) A bad

44. _____ has now evolved to be one of the most popular automated tools for unethical hacking.
(a) Automated apps (b) Database software
(c) Malware (d) Worms

45. _____ is the technique used in business organizations and firms to protect IT assets.
(a) Ethical hacking (b) Unethical hacking
(c) Fixing bugs (d) Internal data-breach

46. The legal risks of ethical hacking include lawsuits due to _____ of personal data.
(a) Stealing (b) Disclosure
(c) Deleting (d) Hacking

47. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?
(a) Know the nature of the organization
(b) Characteristics of work done in the firm
(c) System and network
(d) Type of broadband company used by the firm

48. After performing _____ the ethical hacker should never disclose client information to other parties.
(a) Hacking (b) Cracking
(c) Penetration testing (d) Exploiting

49. _____ is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.
(a) Social ethics (b) Ethics in cyber-security
(c) Corporate ethics (d) Ethics in black hat hacking

50. _____ helps to classify arguments and situations, better understand a cyber-crime and helps to determine appropriate actions.
(a) Cyber-ethics (b) Social ethics
(c) Cyber-bullying (d) Corporate behavior

51. A penetration tester must identify and keep in mind the _____ requirements of a firm while evaluating the security postures.
(a) privacy and security (b) rules and regulations
(c) hacking techniques (d) ethics to talk to seniors

52. Network layer firewall works as a _____
(a) Frame filter (b) Packet filter
(c) Content filter (d) Virus filter

53. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____
(a) Chock point (b) Meeting point
(c) Firewall point (d) Secure point

54. A proxy firewall filters at _____
(a) Physical layer (b) Data link layer
(c) Network layer (d) Application layer

55. A firewall needs to be _____ so that it can grow proportionally with the network that it protects.
(a) Robust (b) Expansive
(c) Fast (d) Scalable

56. A stateful firewall maintains a _____ which is a list of active connections.
(a) Routing table (b) Bridging table
(c) State table (d) Connection table

57. There are _____ types of computer virus.
(a) 5 (b) 7
(c) 10 (d) 12

58. Which of the following is not a type of virus?
(a) Boot sector (b) Polymorphic
(c) Multipartite (d) Trojans

59. A computer _____ is a malicious code which self-replicates by copying itself to other programs.
(a) Program (b) Virus
(c) Application (d) Worm

60. Which of them is not an ideal way of spreading the virus?
(a) Infected website (b) Emails
(c) Official Antivirus CDs (d) USBs

61. _____ gets installed & stays hidden in your computer's memory. It stays involved to the specific type of files which it infects.
(a) Boot Sector Virus (b) Direct Action Virus
(c) Polymorphic Virus (d) Multipartite Virus

62. _____ is also known as cavity virus.
(a) Non-resident virus (b) Overwrite Virus
(c) Polymorphic Virus (d) Space-filler Virus

63. The _____ can cost you money, by sending text messages from your mobile phone numbers.
(a) IM - Trojans (b) Backdoor Trojans
(c) SMS Trojan (d) Ransom Trojan

64. USENET falls under which category of public key sharing?
(a) Public announcement
(b) Publicly available directory
(c) Public-key authority
(d) Public-key certificates

65. In cryptography, what is cipher?
(a) Algorithm for performing encryption and decryption
(b) Encrypted message
(c) Both algorithm for performing encryption and decryption and encrypted message
(d) Decrypted message

66. In asymmetric key cryptography, the private key is kept by _____
(a) Sender
(b) Receiver
(c) Sender and receiver
(d) All the connected devices to the network

67. What is data encryption standard (DES)?
(a) Block cipher (b) Stream cipher
(c) Bit cipher (d) Byte cipher

68. Cryptographic hash function takes an arbitrary block of data and returns _____
(a) Fixed size bit string
(b) Variable size bit string
(c) Both fixed size bit string and variable size bit string
(d) Variable sized byte string

69. Which network topology requires a central controller or hub?
(a) Star (b) Mesh
(c) Ring (d) Bus

70. _____ topology requires a multipoint connection.
(a) Star (b) Mesh
(c) Ring (d) Bus

71. Data communication system within a building or campus is_____
(a) LAN (b) WAN
(c) MAN (d) PAN

72. WAN stands for _____
(a) World Area Network (b) Wide Area Network
(c) Web Area Network (d) Web Access Network

73. _____ is the multiplexing technique that shifts each signal to a different carrier frequency.
(a) FDM (b) TDM
(c) Both FDM & TDM (d) PDM

74. Two devices are in network if _____
(a) A process in one device is able to exchange information with a process in another device
(b) A process is running on both devices
(c) PIDs of the processes running of different devices are same
(d) A process is active and another is inactive

75. Bluetooth is an example of _____
(a) Personal area network (b) Local area network
(c) Virtual private network (d) Wide area network

76. Network congestion occurs _____
(a) In case of traffic overloading
(b) When a system terminates
(c) When connection between two nodes terminates
(d) In case of transfer failure

77. The keys used in cryptography are
(a) Secret key (b) Private key
(c) Public key (d) All of them

78. CHAP stands for?
(a) Challenge Handshake authentication protocol
(b) Challenge Hardware authentication protocol
(c) Circuit Hardware authentication protocol
(d) Circuit Handshake authentication protocol

79. The information that gets transformed in encryption is _____
(a) Plain text (b) Parallel text
(c) Encrypted text (d) Decrypted text

80. Network layer firewall works as a _____
(a) Frame filter (b) Packet filter
(c) Signal filter (d) Content filter

81. WPA2 is used for security in _____
(a) ethernet (b) bluetooth
(c) wi-fi (d) e-mail

82. Pretty good privacy (PGP) is used in _____
(a) browser security (b) email security
(c) FTP security (d) wifi security

83. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?
(a) CDMA (b) CSMA/CA
(c) ALOHA (d) CSMA/CD

84. What is Wired Equivalent Privacy (WEP)?
(a) Security algorithm for ethernet
(b) Security algorithm for wireless networks
(c) Security algorithm for usb communication
(d) Security algorithm for emails

85. What is WPA?
(a) Wi-fi protected access (b) Wired protected access
(c) Wired process access (d) Wi-fi process access

86. An interconnected collection of piconet is called _____
(a) Scatternet (b) Micronet
(c) Mininet (d) Multinet

87. Which one of the following can be considered as the class of computer threats?
(a) Dos Attack (b) Phishing
(c) Soliciting (d) Both A and C

88. _____ is a type of software designed to help the user's computer detect viruses and avoid them.
(a) Malware (b) Adware
(c) Antivirus (d) Both B and C

89. Which one of the following is a type of antivirus program?
(a) Quick heal (b) Mcafee
(c) Kaspersky (d) All of the above

90. Which one of the following is actually considered as the first computer virus?
(a) Sasser (b) Blaster
(c) Creeper (d) Both A and C

91. Code Red is a type of _____
(a) An Antivirus Program (b) A photo editing software
(c) A computer virus (d) A video editing software

92. Which one of the following is also referred to as malicious software?
(a) Maliciousware (b) Badware
(c) Ilegalware (d) Malware

93. Sec ure Hash Algorithm 1 (SHA-1) has a message digest of:
(a) 160-bits (b) 512-bits
(c) 628-bits (d) 820-bits

94. In message confidentiality, the transmitted message must make sense to only intended:
(a) Receiver (b) Sender
(c) Modular (d) Translator

95. Hash function guarantees the integrity of a message. It guarantees that the message has not been:
(a) Replaced (b) Over view
(c) Changed (d) Violated

96. A digital signature needs a:
(a) Shared-key system (b) Private key system
(c) Secret key (d) Public key system

97. A session symmetric key between two parties is used:
(a) Multiple time (b) Twice
(c) Only once (d) Conditions dependent

98. Encryption and decryption provide secrecy or confidentiality, but not provide:
(a) Authentication (b) Privacy
(c) Integrity (d) Modularity

99. MAC stands for:
(a) Message Arbitrary Connection
(b) Message Authentication Control
(c) Message Authentication Code
(d) Message Authentication Cipher

100. The digest created by a hash function is normally called as:
(a) Modify Authentication Connection
(b) Message Authentication Control
(c) Message Authentication Cipher
(d) Modification Detection Code (MDC)

101. When the data must arrive at the receiver exactly as they were sent, it is called:
(a) Message confidentiality (b) Message integrity
(c) Message splashing (d) Message binding

102. In message integrity, Secure Hash Algorithm (SHA-1) hash algorithms create on N-bit message, digest of a message of:
(a) 512 bit blocks (b) 210 bit blocks
(c) 1510 bit blocks (d) 2020 bit blocks

103. IP security (IPSec) is a collection of protocols designed by the IETF to provide security for a packet at the:
(a) Data link (b) Network
(c) Transport (d) None

104. A packet-filter firewall filters at the ___ or ___ layer.
(a) Network; Application (b) Network; Transport
(c) Transport; Application (d) None of the above

105. Which of the following attacks is threatening integrity?
(a) Traffic analysis (b) Denial of Service
(c) Masquerading (d) None of the above

106. In which of the following cryptographies, the same key is used by the sender and the receiver?
(a) Asymmetric key (b) Public key
(c) Symmetric key (d) None of the above

107. Which among the following can provide authentication, integrity, and non-repudiation for a message?
(a) Compression (b) Digital Signature
(c) Encryption/decryption (d) None of the above

108. In which of the following cryptographies, everyone has access to everyone's public key?
(a) Symmetric-key (b) Secret key
(c) Asymmetric-key (d) None of these

109. After a message is encrypted, its called ___

(a) plaintext (b) ciphertext

(c) crypto text (d) none

110. In the asymmetric key method used for confidentiality, which key is publicly known?

(a) Encryption key only (b) Decryption key only

(c) Both keys (d) None

111. The RSA algorithm for confidentiality uses which of the following cryptographies?

(a) Substitution (b) Symmetric key

(c) Asymmetric key (d) None

112. You need to create an access list that will prevent hosts in the network range of 192.168.160.0 to 192.168.191.160. Which of the following lists will you use?

(a) Access-list 10 deny 192.168.160.0 0.0.192.255

(b) Access-list 10 deny 192.168.168.0 0.0.31.255

(c) Access-list 10 deny 192.168.160.0 0.0.31.255

(d) Access-list 10 deny 192.168.160.0 0.0.31.255

113. Which router command allows you to view the entire contents of all access lists?

(a) Router # show interface

(b) Router > show if interface

(c) Router # show access lists

(d) Router > show all access lists

114. A high-profile company is experiencing attacks. The network administrator wants to collect data on attackers before taking legal action. What should be implemented?

(a) A DMZ (Demilitarized zone)

(b) A honey pot

(c) A subnet

(d) Firewall

115. Wireless Application Protocol (WAP) has several layers. Which of the following is the security layer?

(a) Wireless Security Layer (WSL)

(b) Wireless Transport Layer (WTL)

(c) Wireless Transport Layer Security (WTLS)

(d) Wireless Security Layer Transport (WSLT)

116. Which among the following is *not* a type of firewall?

(a) Stateful Query (b) Application Proxy

(c) Static packet filtering (d) Symmetric Proxy

117. One way to limit hostile sniffing on a LAN is by installing:

(a) An ethernet access point (b) A repeater

(c) An ethernet hub (d) A CDSU/DSU

118. Challenge-response authentication can be done using:

(a) Symmetric key ciphers (b) Asymmetric key ciphers

(c) Keyed hash functions (d) All of the above

119. If a packet arrives with an M-bit value '1' and fragmentation offset value '0', then it comes under which fragment?

(a) First (b) Middle

(c) Last (d) All of the above

120. AES is a round cipher based on the Rijndael Algorithm that uses a 128-bit block of data. AES has three different configurations.

With a key size of 128 bits, ___ rounds.

With a key size of 192 bits, ___ rounds.

With a key size of 256 bits, ___ rounds.

(a) 8, 10, 12 (b) 10, 12, 14

(c) 12, 14, 16 (d) 10, 15, 25

121. Data Encryption Techniques are particularly used for which of the following?

(a) Protecting data in Data Communication System

(b) Reduce Storage Space Requirement

(c) Enhances Data Integrity

(d) Decreases Data Integrity

122. Which of the following is the example of a layer that is absent in broadcast networks?

(a) Physical layer (b) Presentation layer

(c) Network layer (d) Application layer

123. The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is known as:

(a) Bit stuffing (b) Piggy backing

(c) Pipelining (d) Broadcasting

124. Using RSA algorithm, what is the value of cipher text C, if the plain text M = 5 and p = 3, q = 11 and d = 7?

(a) 5 (b) 27

(c) 34 (d) 26

125. Encryption and Decryption is the responsibility of ___ Layer

(a) Physical (b) Network

(c) Application (d) Datalink

126. Using the RSA public key cryptosystem, if p = 13, q = 31 and d = 7, then the value of e is

(a) 101 (b) 102

(c) 103 (d) 104

127. Which of the following statements is incorrect?

(a) Symmetric key algorithms are used in contemporary cryptography to encrypt and decrypt data using the same key.

(b) Using the same key, one cannot decrypt the cipher DES (Data Encryption Standard).

(c) The AES (Advanced Encryption Standard) cryptosystem allows variable key lengths of 256 bits and 124 bits.

(d) Public key algorithms use two different keys for Encryption and Decryption.