

Internet Security

Multiple Choice Question & Answers:-

1. Message_____ means that the data must arrive at the receiver exactly as sent.

- A) confidentiality
- B) integrity
- C) authentication
- D) none of the above

Answer:B

2. Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.

- A) confidentiality
- B) integrity
- C) authentication
- D) none of the above

Answer:C

3. A(n) _____ function creates a message digest out of a message.

- A) encryption

- B) decryption
- C) hash
- D) none of the above

Answer:C

4. The secret key between members needs to be created as a _____ key when two members contact KDC.

- A) public
- B) session
- C) complimentary
- D) none of the above

Answer:B

5. The _____ criterion ensures that a message cannot easily be forged.

- A) one-wayness
- B) weak-collision-resistance
- C) strong-collision-resistance
- D) none of the above

Answer:B

6. A(n) _____ is a trusted third party that assigns a symmetric key to two parties.

- A) KDC
- B) CA
- C) KDD
- D) none of the above

Answer:A

7. A witness used in entity authentication is _____.

- A) something known
- B) something possessed
- C) something inherent
- D) all of the above

Answer:D

8. A _____ message digest is used as an MDC.

- A) keyless
- B) keyed
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:A

9. A(n)_____ creates a secret key only between a member and the center.

- A) CA
- B) KDC
- C) KDD
- D) none of the above

Answer:B

10. _____ means to prove the identity of the entity that tries to access the system's resources.

- A) Message authentication
- B) Entity authentication
- C) Message confidentiality
- D) none of the above

Answer:B

11. A _____ signature is included in the document; a _____ signature is a separate entity.

- A) conventional; digital
- B) digital; digital
- C) either (a) or (b)

D) neither (a) nor (b)

Answer:A

12. If _____ is needed, a cryptosystem must be applied over the scheme.

- A) integrity
- B) confidentiality
- C) nonrepudiation
- D) authentication

Answer:B

13. Digital signature provides _____.

- A) authentication
- B) nonrepudiation
- C) both (a) and (b)
- D) neither (a) nor (b)

Answer:C

14. Digital signature cannot provide _____ for the message.

- A) integrity

- B) confidentiality
- C) nonrepudiation
- D) authentication

Answer:B

15. To authenticate the data origin, one needs a(n) _____.

- A) MDC
- B) MAC
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:A

16. A(n) _____ can be used to preserve the integrity of a document or a message.

- A) message digest
- B) message summary
- C) encrypted message
- D) none of the above

Answer:A

17. Challenge-response authentication can be done using _____.

- A) symmetric-key ciphers
- B) asymmetric-key ciphers
- C) keyed-hash functions
- D) all of the above

Answer:D

18. The _____ criterion ensures that we cannot find two messages that hash to the same digest.

- A) one-wayness
- B) weak-collision-resistance
- C) strong-collision-resistance
- D) none of the above

Answer:C

19. A digital signature needs a(n) _____ system.

- A) symmetric-key
- B) asymmetric-key
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:B

20. A(n) _____ is a federal or state organization that binds a public key to an entity and issues a certificate.

- A) KDC
- B) Kerberos
- C) CA
- D) none of the above

Answer:C

21. Message _____ means that the sender and the receiver expect privacy.

- A) confidentiality
- B) integrity
- C) authentication
- D) none of the above

Answer:A

22. In _____ authentication, the claimant proves that she knows a secret without actually sending it.

- A) password-based
- B) challenge-response
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:B

23. In _____, a claimant proves her identity to the verifier by using one of the three kinds of witnesses.

- A) message authentication
- B) entity authentication
- C) message confidentiality
- D) message integrity

Answer:B

24. The _____ criterion states that it must be extremely difficult or impossible to create the message if the message digest is given.

- A) one-wayness
- B) weak-collision-resistance
- C) strong-collision-resistance
- D) none of the above

Answer:A

25. A(n) _____ is a hierarchical system that answers queries about key certification.

- A) KDC

- B) PKI
- C) CA
- D) none of the above

Answer:C

26. _____ means that a sender must not be able to deny sending a message that he sent.

- A) Confidentiality
- B) Integrity
- C) Authentication
- D) Nonrepudiation

Answer:D

27. A hash function must meet _____ criteria.

- A) two
- B) three
- C) four
- D) none of the above

Answer:B

28. _____ is a popular session key creator protocol that requires an authentication server and a ticket-granting server.

- A) KDC
- B) Kerberos
- C) CA
- D) none of the above

Answer:B

29. Password-based authentication can be divided into two broad categories: _____ and _____.

- A) fixed; variable
- B) time-stamped; fixed
- C) fixed; one-time
- D) none of the above

Answer:C

30. _____ operates in the transport mode or the tunnel mode.

- A) IPSec
- B) SSL
- C) PGP
- D) none of the above

Answer:A

31. IKE creates SAs for _____.

- A) SSL
- B) PGP
- C) IPSec
- D) VP

Answer:C

32. _____ provides either authentication or encryption, or both, for packets at the IP level.

- A) AH
- B) ESP
- C) PGP
- D) SSL

Answer:B

33. One security protocol for the e-mail system is _____.

- A) IPSec
- B) SSL
- C) PGP
- D) none of the above

Answer:C

34.protocol is normally HTTP.

- A) SSL
- B) TLS
- C) either (a) or (b)
- D) both (a) and (b)

Answer:

35. IKE is a complex protocol based on _____ other protocols.

- A) two
- B) three
- C) four
- D) five

Answer:B

36. IPSec defines two protocols: _____ and _____.

- A) AH; SSL
- B) PGP; ESP

- C) AH; ESP
- D) all of the above

Answer:A

37. In the _____ mode, IPSec protects information delivered from the transport layer to the network layer.

- A) transport
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:A

38. _____ is the protocol designed to create security associations, both inbound and outbound.

- A) SA
- B) CA
- C) KDC
- D) IKE

Answer:D

39. A _____ network is used inside an organization.

- A) private
- B) public
- C) semi-private
- D) semi-public

Answer:A

40. SSL provides _____.

- A) message integrity
- B) confidentiality
- C) compression
- D) all of the above

Answer:D

41. The Internet authorities have reserved addresses for _____.

- A) intranets
- B) internets
- C) extranets
- D) none of the above

Answer:D

42. An _____ is a network that allows authorized access from outside users.

- A) intranet
- B) internet
- C) extranet
- D) none of the above

Answer:C

43. _____ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.

- A) IPSec
- B) SSL
- C) PGP
- D) none of the above

Answer:A

44. IKE uses _____.

- A) Oakley
- B) SKEME
- C) ISAKMP
- D) all of the above

Answer:D

45. IPSec uses a set of SAs called the _____.

- A) SAD
- B) SAB
- C) SADB
- D) none of the above

Answer:C

46. An _____ is a private network that uses the Internet model.

- A) intranet
- B) internet
- C) extranet
- D) none of the above

Answer:A

47. _____ is actually an IETF version of _____.

- A) TLS; TSS
- B) SSL; TLS
- C) TLS; SSL

D) SSL; SLT

Answer:C

48. In _____, there is a single path from the fully trusted authority to any certificate.

- A) X509
- B) PGP
- C) KDC
- D) none of the above

Answer:A

49. The combination of key exchange, hash, and encryption algorithms defines a _____ for each SSL session.

- A) list of protocols
- B) cipher suite
- C) list of keys
- D) none of the above

Answer:B

50. A _____ provides privacy for LANs that must communicate through the global Internet.

- A) VPP

- B) VNP
- C) VNN
- D) VPN

Answer:D

51. _____ uses the idea of certificate trust levels.

- A) X509
- B) PGP
- C) KDC
- D) none of the above

Answer:B

52. IPSec in the _____ mode does not protect the IP header.

- A) transport
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:A

53. _____ provides privacy, integrity, and authentication in e-mail.

- A) IPSec
- B) SSL
- C) PGP
- D) none of the above

Answer:C

54. In _____, there can be multiple paths from fully or partially trusted authorities.

- A) X509
- B) PGP
- C) KDC
- D) none of the above

Answer:B

55. _____ provides authentication at the IP level.

- A) AH
- B) ESP
- C) PGP
- D) SSL

Answer:A

56. In _____, the cryptographic algorithms and secrets are sent with the message.

- A) IPSec
- B) SSL
- C) TLS
- D) PGP

Answer:D

57. _____ is designed to provide security and compression services to data generated from the application layer.

- A) SSL
- B) TLS
- C) either (a) or (b)
- D) both (a) and (b)

Answer:D

58. _____ provide security at the transport layer.

- A) SSL
- B) TLS
- C) either (a) or (b)
- D) both (a) and (b)

Answer:D

59. The _____ mode is normally used when we need host-to-host (end-to-end) protection of data.

- A) transport
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:A

60. In the _____ mode, IPSec protects the whole IP packet, including the original IP header.

- A) transport
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

Answer:B

61. _____ was invented by Phil Zimmerman.

- A) IPSec
- B) SSL

- C) PGP
- D) none of the above

Answer:C

62. A _____ layer security protocol provides end-to-end security services for applications.

- A) data link
- B) network
- C) transport
- D) none of the above

Answer:C

63. In PGP, to exchange e-mail messages, a user needs a ring of _____ keys.

- A) secret
- B) public
- C) either (a) or (b)
- D) both (a) and (b)

Answer:B

64. A user needs to send the server some information. The request line method is _____.

- A) OPTION
- B) PATCH
- C) POST
- D) none of the above

Answer:C

65. In a URL, the _____ is the client-server program used to retrieve the document.

- A) path
- B) protocol
- C) host
- D) none of the above

Answer:B

66. A _____ document is created by a Web server whenever a browser requests the document.

- A) static
- B) dynamic
- C) active
- D) none of the above

Answer:B

67. One way to create an active document is to use _____.

- A) CGI
- B) Java stand-alone programs
- C) Java applets
- D) none of the above

Answer:C

68. A cookie is made by the _____ and eaten by the _____.

- A) client; client
- B) client; server
- C) server; server
- D) none of the above

Answer:C

69. A _____ document is a fixed-content document that is created and stored in a server. The client can get a copy of the document only.

- A) static
- B) dynamic
- C) active
- D) none of the above

Answer:A

70. The _____ is a standard for specifying any kind of information on the Internet.

- A) URL
- B) ULR
- C) RLU
- D) none of the above

Answer:A

71. _____ is a repository of information linked together from points all over the world.

- A) The WWW
- B) HTTP
- C) HTML
- D) none of the above

Answer:A

72. Which of the following is present in both an HTTP request line and a status line?

- A) HTTP version number
- B) URL

- C) status code
- D) none of the above

Answer:A

73. Active documents are sometimes referred to as _____ dynamic documents.

- A) client-site
- B) server-site
- C) both a and b
- D) none of the above

Answer:A

74. HTTP uses the services of _____ on well-known port 80.

- A) UDP
- B) IP
- C) TCP
- D) none of the above

Answer:C

75. Dynamic documents are sometimes referred to as _____ dynamic documents.

- A) client-site
- B) server-site
- C) both a and b
- D) none of the above

Answer:B

76. For many applications, we need a program or a script to be run at the client site. These are called _____ documents.

- A) static
- B) dynamic
- C) active
- D) none of the above

Answer:C

77. In HTTP, a _____ server is a computer that keeps copies of responses to recent requests.

- A) regular
- B) proxy
- C) both a and b
- D) none of the above

Answer:B

78. The HTTP request line contains a _____ method to get information about a document without retrieving the document itself.

- A) HEAD
- B) POST
- C) COPY
- D) none of the above

Answer:A

79. A response message always contains _____.

- A) a header and a body
- B) a request line and a header
- C) a status line and a header
- D) none of the above

Answer:C

80. In a URL, an optional _____ can be inserted between the host and the path, and it is separated from the host by a colon.

- A) path
- B) protocol
- C) host
- D) none of the above

Answer:D

81. An applet is _____ document application program.

- A) a static
- B) an active
- C) a passive
- D) a dynamic

Answer:B

82. The documents in the WWW can be grouped into _____ broad categories.

- A) two
- B) three
- C) four
- D) none of the above

Answer:B

83. _____ is a language for creating Web pages.

- A) HTTP
- B) HTML

- C) FFTP
- D) none of the above

Answer:B

84. _____ is a technology that creates and handles dynamic documents.

- A) GIC
- B) CGI
- C) GCI
- D) none of the above

Answer:B

85. The HTTP request line contains a _____ method to request a document from the server.

- A) GET
- B) POST
- C) COPY
- D) none of the above

Answer:A

86. In a _____ connection, the server leaves the connection open for more requests after sending a response.

- A) persistent
- B) nonpersistent
- C) both a and b
- D) none of the above

Answer:A

87. An HTTP request message always contains _____.

- A) a header and a body
- B) a request line and a header
- C) a status line, a header, and a body
- D) none of the above

Answer:B

88. In a _____ connection, one TCP connection is made for each request/response.

- A) persistent
- B) nonpersistent
- C) both a and b
- D) none of the above

Answer:B

89. In a URL, the _____ is the full name of the file where the information is located.

- A) path
- B) protocol
- C) host
- D) none of the above

Answer:A

90. In a URL, the _____ is the computer on which the information is located.

- A) path
- B) protocol
- C) host
- D) none of the above

Answer:C

91. HTTP version 1.1 specifies a _____ connection by default.

- A) persistent
- B) nonpersistent
- C) both a and b
- D) none of the above

Answer:A

92. In HTTP, the first line in a request message is called a _____ line; the first line in the response message is called the _____ line.

- A) request; response
- B) response; request
- C) response; status
- D) none of the above

Answer:D

93. The WWW today is a _____ client-server service, in which a client using a browser can access a service using a server.

- A) limited
- B) vast
- C) distributed
- D) none of the above

Answer:C