Dr.G.R.Damodaran College of Science

(Autonomous, affiliated to the Bharathiar University, recognized by the UGC)Re-accredited at the 'A' Grade Level by the **NAAC** and ISO 9001:2008 Certified
CRISL rated 'A' (TN) for MBA and MIB Programmes

II MSc IT [2016-2018]
Semester III
Core: Network Security - 363C
Multiple Choice Questions.

1. Security in enterprise systems that are connected in network share _____.
   A. attacks.
   B. confidential information.
   C. threats.
   D. uncovered vulnerabilities.
   ANSWER: B

2. The goals of secure computing include _____.
   A. confidentiality.
   B. integrity.
   C. availability.
   D. all the above.
   ANSWER: D

3. Which of the following is a computer based system that has three separate but valuable components?
   A. Hardware.
   B. Attacks.
   C. Integrity.
   D. Vulnerabilities.
   ANSWER: A

4. A _____ is a weakness in the security system.
   A. threat.
   B. software.
   C. vulnerability.
   D. confidentiality.
   ANSWER: C

5. A _____ to a computing system is a set of circumstances that has the potential to cause loss or harm.
   A. data.
   B. information.
   C. threat.
   D. integrity.
   ANSWER: C

6. A human who exploits vulnerability perpetrates an _____ on the system.

A. control.
B. data.
C. security.
D. attack.
ANSWER: D

7. IETF means _____.
A. Internet Executing Task Force.
B. Indian Engineers Task Force.
C. Internet Engineering Task Force.
D. Indian Executing Task Force.
ANSWER: C

8. A threat is _____ by control of vulnerability.
A. blocked.
B. allowed.
C. released.
D. suspended.
ANSWER: A

9. _____ processes the input elements continously, producing output one element at a time.
A. block cipher.
B. stream cipher.
C. key cipher.
D. bit cipher.
ANSWER: B

10. How many rounds does the Feistel strucutre have?
A. 16.
B. 18.
C. 20.
D. 21.
ANSWER: A

11. A _____ studies encryption and encrypted messages, hoping to find the hidden meanings.
A. cryptographer.
B. cryptanalyst.
C. decoder.
D. cryptographer.
ANSWER: B

12. The generic name for the collection of tools designed to protect data and to thwart hackers is _____.
A. network security.
B. computer security.
C. internet security.
D. data security.
ANSWER: B

13. The block in AES is copied to _____ array which is modified at each stage of encryption and

decryption.
A. block.
B. state.
C. message.
D. stream.
ANSWER: B

14. Choose from the following the transmitted ciphertext in simple model of symmetric encryption.
A. Y = D[K,X].
B. Y = E[K,X].
C. Y = E[X].
D. Y = D[K].
ANSWER: B

15. _____ ensures that computer related assets are accessed only by authorized parties.
A. Confidentiality.
B. Integrity.
C. Availability.
D. All the above
ANSWER: A

16. _____ is sometimes called secrecy or privacy.
A. Interruption.
B. Confidentiality.
C. Fabrication.
D. Motivation.
ANSWER: B

17. Availability is sometimes known by its opposite, _____.
A. secrecy.
B. privacy.
C. denial of service.
D. secrecy of serve
ANSWER: C

18. _____ is a program that has a secret entry point.
A. Trojan horse.
B. Virus.
C. Trapdoor.
D. Information leaks.
ANSWER: C

19. Which of the following is a 3DES function?
A. Encrypt-Decrypt-Decrypt.
B. Encrypt-Decrypt-Encrypt.
C. Decrypt-Encrypt-Encrypt.
D. Encrypt-Decrypt-Decrypt.
ANSWER: B

20. IDS stands for _____.
A. intrusion detection system.

B. instruction detection system.
C. information detection system
D. instruction document section
ANSWER: A

21. The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts is referred as _____.
A. Traffic Padding.
B. Routing control.
C. Access control.
D. Notarization.
ANSWER: A

22. An encryption scheme that does not require the use of a key is called a _____.
A. plain text.
B. key cipher.
C. keyless cipher.
D. cipher text
ANSWER: C

23. A permutation is a _____ of the elements of a sequence
A. reordering.
B. scramble.
C. arrangement.
D. prefix
ANSWER: A

24. A _____ cipher encrypts a group of plaintext symbols as one block.
A. stream.
B. key.
C. column.
D. block.
ANSWER: D

25. AES is a block cipher of block size _____ bits.
A. 128.
B. 192.
C. 256.
D. 312.
ANSWER: A

26. Which of the following is not a type of Active attack?
A. Replay.
B. Message content.
C. Masquerade.
D. Denial of service.
ANSWER: B

27. A certificate is signed by _____.
A. certificate authority.
B. hacker.

C. trustee.
D. intruder
ANSWER: A

28. The block size of DES is _____ bits
A. 64.
B. 128.
C. 312.
D. 412.
ANSWER: A

29. Design of both AES and DES are _____.
A. open.
B. closed.
C. both open and closed.
D. none of the above.
ANSWER: A

30. NBS stands for _____.
A. National Board of Standards.
B. National Bureau of Standards.
C. National Board of Security.
D. National Bureau of Security.
ANSWER: B

31. An arbiter or distributer of information is known as _____.
A. Trusted third party.
B. Sender.
C. Receiver.
D. Third party.
ANSWER: A

32. Which of the following is the ability to limit and control the access to host systems and applications via communications links?
A. Confidentiality.
B. Availability.
C. Access control.
D. Nonrepudiation.
ANSWER: C

33. _____ is the general name for unanticipated or undesired effects in programs or program parts, caused by an agent intent on damage
A. Malicious code.
B. Virus.
C. Buffer.
D. Domain
ANSWER: A

34. A _____ is an unauthorized program that performs functions unknown by the user
A. virus.
B. malicious code.

C. Trojan horse.
D. agent
ANSWER: C

35. Malicious code is also known as _____ program.
A. threat.
B. rogue.
C. resident.
D. transient.
ANSWER: B

36. A virus that can change its appearance is called a _____ virus.
A. mono.
B. tetra.
C. poly.
D. polymorphic.
ANSWER: D

37. S-box refers to _____.
A. standard byte.
B. substitute bit.
C. standard box.
D. substitution box.
ANSWER: D

38. What is the value of ciphertext in stream cipher if the input to plaintext and key stream is 01101100 and 01101100?
A. 1010101.
B. 1111000.
C. 10100000.
D. 01110101.
ANSWER: C

39. A _____ is a program that can replicate itself and send copies from computer to computer across network connections.
A. Worm.
B. Trapdoors.
C. Denial of Service.
D. FTP Trojans
ANSWER: A

40. A _____applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
A. Stateful inspection firewall.
B. Packet filtering firewall.
C. Application proxy firewall.
D. Circuit-level proxy firewall.
ANSWER: B

41. Which of the following assures that information and programs are changed only in a specified and authorized manner?

A. Data confidentiality.
B. Privacy.
C. Data Integrity.
D. System Integrity.
ANSWER: C

42. Which of the following attack is easiest to defend?
A. Ciphertext only.
B. Chosen ciphertext.
C. Chosen plaintext.
D. Known plaintext.
ANSWER: A

43. Which of the following criteria is used to validate that a sequence of numbers is random?
A. Irregular distribution of bits.
B. Dependence.
C. Partial distribution of bits.
D. Independence.
ANSWER: D

44. Which of the following random number generator takes the input as seed value?
A. PRF.
B. PRNG.
C. TRNG.
D. FRNG.
ANSWER: C

45. Confidentiality with asymmetric-key cryptosystem has its own _____.
A. system.
B. data.
C. problems.
D. issues.
ANSWER: C

46. SHA-l has a message digest of _____.
A. 512.
B. 160.
C. 628.
D. 820.
ANSWER: B

47. Message authentication is a service beyond _____.
A. Message Integrity.
B. Message Confidentiality.
C. Message Splashing.
D. Message Sending.
ANSWER: A

48. In Message Confidentiality, transmitted message must make sense to only intended _____.
A. sender.
B. third party.

C. receiver.
D. translator.
ANSWER: C

49. A hash function guarantees integrity of a message. It guarantees that message has not be _____.
A. replaced.
B. changed.
C. removed.
D. left.
ANSWER: B

50. A digital signature needs a _____.
A. private-key system.
B. shared-key system.
C. public-key system.
D. all of the above.
ANSWER: C

51. A session symmetric key between two parties is used _____.
A. only once.
B. twice.
C. multiple items.
D. depends on situation.
ANSWER: A

52. Encryption and decryption provide secrecy, or confidentiality, but not _____.
A. Authentication.
B. Keys.
C. Frames.
D. Integrity.
ANSWER: D

53. MAC stands for _____.
A. message authentication control.
B. message authentication connection.
C. message authentication cipher.
D. message authentication code.
ANSWER: D

54. Message confidentiality uses_____.
A. Cipher Text.
B. Plain Text.
C. Asymmetric-Key.
D. Symmetric-Key.
ANSWER: C

55. _____ is called as a good collection of research papers and articles of network security.
A. Honeybees.
B. HoneyPots.
C. HoneyTank.
D. Beehive.

ANSWER: B

56. Expansion for SSL is _____.
A. Secure Socket Layer.
B. Software Security Layer.
C. System Software Layer.
D. Security System Layer.
ANSWER: A

57. A sender must not be able to deny sending a message that he or she, in fact, did send, is known as _____.
A. Message Integrity.
B. Message Confidentiality.
C. Message Nonrepudiation.
D. Message Sending.
ANSWER: C

58. Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not _____.
A. joined.
B. separate.
C. submit.
D. authenticated.
ANSWER: D

59. Heart of Data Encryption Standard (DES), is the _____.
A. Cipher.
B. DES function.
C. Rounds.
D. Encryption.
ANSWER: B

60. For RSA to work, value of P must be less than value of _____.
A. n.
B. p.
C. r.
D. q.
ANSWER: A

61. Cryptography, a word with Greek origins, means _____.
A. Secret Writing.
B. Corrupting Data.
C. Open Writing.
D. Closed Writing.
ANSWER: A

62. Who designed Advanced Encryption Standard (AES)?
A. IBM.
B. National Institute of Standards and Technology
C. HP.
D. Intel.

ANSWER: B

63. CFB stands for _____.
A. Cipher Feedback Mode.
B. Cipher Fetch Board Mode.
C. Cipher Fear Board Mode.
D. Cyber Feedback Mode.
ANSWER: A

64. RSA stands for _____.
A. Rivest, Shamir, Adleman.
B. Roger, Shamir, Adrian.
C. Robert, Shamir, Anthoney.
D. Rivest, Shaw, Adleman.
ANSWER: A

65. SSL divides data into blocks of _____.
A. 2 * 20.
B. 2 * 6.
C. 2 * 24.
D. 2 * 14.
ANSWER: D

66. Which of the protocols provide security at application layer?
A. Handshake Protocol.
B. Alert Protocol.
C. Record Protocol.
D. Pretty Good Privacy.
ANSWER: D

67. A proxy firewall filters at the _____.
A. physical layer.
B. data link layer.
C. network layer.
D. application layer.
ANSWER: D

68. _____ is a piece of software that can infect other programs by modifying them.
A. Virus.
B. DoS.
C. Kerberos.
D. Firewall.
ANSWER: A

69. A packet filter firewall filters at the _____.
A. application or transport layer.
B. network or transport layer.
C. data link layer.
D. physical layer.
ANSWER: B

70. Kerberos implements both authentication and access authorization by means of capabilities called _____.
A. tokens.
B. tickets.
C. server.
D. distribution
ANSWER: B

71. Which of the following is an alternative for MAC?
A. two-way hash function.
B. three-way hash function.
C. simple hash function.
D. one-way hash function.
ANSWER: D

72. Which of the following port number is used for HTTP?
A. 73.
B. 80.
C. 82.
D. 64.
ANSWER: B

73. What is the expansion for KDC?
A. Key Distribution Center.
B. Key Data Center.
C. Knowledge Distribution Center.
D. Knowledge Data Center
ANSWER: A

74. Exhaustive attack also known as _____.
A. malicious.
B. salami.
C. attack code.
D. brute force.
ANSWER: D

75. Which of the following port number is used for HTTPS?
A. 321.
B. 343.
C. 443.
D. 258.
ANSWER: C

76. Which of the following algorithm is not used in TLS?
A. Fortezza.
B. RSA.
C. DES.
D. DSS.
ANSWER: A

77. Which of the following is an important SSL state?

A. shared key.
B. secret key.
C. password.
D. session.
ANSWER: D

78. Which of the following is a parameter of the connection state?
A. Master secret.
B. Server write key.
C. Peer certificate.
D. Session identifier.
ANSWER: B

79. Using the RSA algorithm, find the value of d when p=17,q=11 and e=7?
A. 12.
B. 23.
C. 32.
D. 48.
ANSWER: B

80. How many registers are there in SHA?
A. 8.
B. 5.
C. 7.
D. 6.
ANSWER: A

81. Which of the following is a primitive root of 353?
A. 6.
B. 3.
C. 4.
D. 7.
ANSWER: B

82. _____ is a key distribution and user authentication service provided by MIT.
A. Ketos.
B. Kerberos.
C. Digital Signature.
D. Denial of Service.
ANSWER: B

83. Information that is delivered as a unit between MAC users is known as _____.
A. Access point.
B. Distribution system.
C. MAC service data unit.
D. MAC protocol data unit.
ANSWER: D

84. The expansion of WAP is _____.
A. Wireless Application Protocol.
B. Wireless Access. Protocol.

C. Wired Application Protocol.
D. Wired Access Protocol.
ANSWER: A

85. Which of the following is the major version of TLS and SSL?
A. 3.
B. 0.
C. 2.
D. 7.
ANSWER: A

86. On satisfying which of the following property a hash function is considered to be strong?
A. fixed length output.
B. second preimage resistant.
C. preimage resistant.
D. collision resistant.
ANSWER: D

87. What is the number of steps required for SHA-256?
A. 80.
B. 64.
C. 35.
D. 48.
ANSWER: B

88. _____ mode of operation is used for AES and 3DES.
A. CCM.
B. CMAC.
C. CMC.
D. MCAC.
ANSWER: B

89. Which of the following algorithm cannot be used for encryption or key exchange?
A. Digital Signature Standard.
B. RSA.
C. Data Encryption Standard.
D. Elliptic Curve Cryptography.
ANSWER: A

90. _____ knows the password of all users and stores them in centralized database.
A. Ticket Server.
B. Authentication Server.
C. Network Server.
D. Password server.
ANSWER: B

91. _____ indicates the date and time at which the ticket was issued.
A. tickets.
B. time.
C. date.
D. timestamp.

ANSWER: D

92. _____ indicates the length of time for which the ticket was valid.
A. timestamp.
B. server.
C. lifetime.
D. client.
ANSWER: C

93. A _____ is a set of managed nodes that share the same Kerberos database.
A. Kerberos principal.
B. Kerberos realms.
C. Kerberos session.
D. Kerberos server.
ANSWER: B

94. How many secure key exchanges are required in kerberos realms if there are N realms?
A. N/2.
B. N/2-1.
C. N-1/2.
D. N(N-1)/2.
ANSWER: D

95. Which of the following is not a technical defeciency but an environment limitations of Kerberos version 4?
A. Double encryption.
B. Interrealm authenticaton.
C. Session keys.
D. Password attacks.
ANSWER: B

96. Which of the following countermeaures is used for the integrity threat in web security?
A. Web proxies.
B. Cryptographic techniques.
C. Encryption.
D. Cryptographic sums.
ANSWER: D

97. An alert protocol takes _____ byte.
A. 2.
B. 1.
C. 0.
D. 3.
ANSWER: B

98. _____ supports local forwarding and remote forwarding.
A. SSL.
B. SSH.
C. TLS.
D. HTTPS.
ANSWER: B

99. _____provides security services between TCP and applications that use TCP.
A. LAN.
B. IP.
C. SSL.
D. X.509.
ANSWER: C

100. Which of the following command indicates that the connection is closed after the record is delivered in HTTP?
A. Connection:exit.
B. Connection:close.
C. Connection:stop.
D. Connection:over.
ANSWER: B

101. Which of the following service is used to support MSDU delivery?
A. Integration.
B. Authentication.
C. Privacy.
D. Deauthentication.
ANSWER: A

102. From the following transition type choose the type that is stationary.
A. No transition.
B. BSS transition.
C. ESS transition.
D. DSS transition.
ANSWER: A

103. Which of the following are the elements of WAP programming model?
A. Time, gateway and server.
B. Client, language and server.
C. Client, gateway and server.
D. Client, language and time.
ANSWER: C

104. WML documents are subdivided into small, well defined units of user interaction called _____.
A. blocks.
B. modules.
C. cards.
D. bits.
ANSWER: C

105. Which of the following transaction classes provides an unreliable datagram service?
A. Class 1.
B. Class 2.
C. Class 0.
D. Class 3.
ANSWER: C

106. What does 'r' represents in WTLS record format?
A. Reserved.
B. Record.
C. Reliable.
D. Remove.
ANSWER: A

107. Choose from the following the second phase of Handshake Protocol.
A. Server authentication and key exchange.
B. Completes the setting up of a secure connection.
C. Client authentication and key exchange.
D. Establish security capabilities.
ANSWER: A

108. Which of the following alphabet repesents the negotiated key used as the pre_master_secret?
A. K.
B. T.
C. B.
D. Z.
ANSWER: D

109. In which phase the random numbers are exchanged in the handshake protocol?
A. Fourth phase.
B. First phase.
C. Third phase.
D. Second phase.
ANSWER: B

110. Which of the following is not encrypted in the WTLS record?
A. Compresed message.
B. MAC.
C. Header.
D. Fragments.
ANSWER: C

111. Choose from the following the service offered by PGP.
A. Secuirty.
B. E-mail compatibility.
C. Message Digest.
D. Decryption.
ANSWER: B

112. Which of the following is mandatory component in the concept of key indentifier in PGP?
A. signature.
B. session key.
C. message.
D. random key.
ANSWER: C

113. WPA refers to _____.
A. World Protected Access.

B. Well Protected Access.
C. Wealth Protected Access.
D. Wi-fi Protected Access.
ANSWER: D

114. Which bit is set if the key appears in the secret key ring?
A. WARNONLY.
B. CONTIG.
C. BUCKSTOP.
D. SIGN.
ANSWER: C

115. Which of the following field assigns trust to public key/user id pair?
A. OWNERTRUST.
B. SIGTRUST.
C. PCKTRUST.
D. KEYLEGIT.
ANSWER: D

116. MIME stands for _____.
A. Multiple Internet Mail Extension.
B. Multi Intranet Module Extended.
C. Multipurpose Internet Mail Extension.
D. Multiplex Internet Module Extension.
ANSWER: C

117. Which of the following describes the data contained in the body with sufficient detail?
A. Content-ID.
B. Content-Description.
C. Content-Type.
D. Content-Transfer-Encoding.
ANSWER: C

118. _____ is used to send large volume of unwanted emails is a malicious function.
A. Worms.
B. Trojen Horse.
C. Exploits.
D. Spammer Programs.
ANSWER: D

119. _____captures keystrokes on a compromised system.
A. Key loggers.
B. Password sending trojans.
C. Flooders.
D. Zombie.
ANSWER: A

120. Choose from the following the subtype of the MIME content type audio.
A. Partial.
B. Mixed
C. Parallel.

D. Basic.
ANSWER: D

121. What terminologies are used in cryptographic algorithms to specify the requirement level in S/MIME?
A. PURPOSE and SHOULD.
B. MUST and CONTENT.
C. MUST and SHOULD.
D. PURPOSE and CONTENT.
ANSWER: C

122. A Digital ID contains _____.
A. Session ID.
B. Owner's public key.
C. Server ID.
D. Owner's private key.
ANSWER: B

123. IEEE 802.11 is a standard for _____.
A. Wireless LAN.
B. LAN.
C. Wirelesss Sensors.
D. Wireless VPN.
ANSWER: A

124. The VeriSign public primary certification authority is referred as _____in Verisign public certificate classes.
A. LRAA.
B. PCA.
C. PIN.
D. IA.
ANSWER: B

125. Who from the following can take a single incoming message , perform the reciptent-specific encryption and forward the message?
A. CLA.
B. TLA.
C. SLA.
D. MLA.
ANSWER: D

126. _____ is used to expand pairwise keys.
A. Pseudo-random function.
B. Random function.
C. Hash function.
D. Aggregate function.
ANSWER: A

127. _____ is a collection of documents describing the key management schemes for use with Ipsec.
A. Other.
B. Authentication Header.

C. Internet key exchange.
D. Architecture.
ANSWER: C

128. Number of rounds used in AES algorithm _____.
A. 9.
B. 16.
C. 10.
D. 15.
ANSWER: A

129. What are the modes supported by the Authentication header and Encapsulating Payload?
A. Transport and Tunnel mode.
B. Tunnel and network mode.
C. Transport and network mode.
D. Only network mode.
ANSWER: A

130. The Security Paramters Index takes _____ bits to identify a security association.
A. 32.
B. 128.
C. 64.
D. 52.
ANSWER: A

131. The term _____ refers to a sequence of SAs through whcih traffic must be processed to provide a desired set of IPsec services.
A. Security Alternate Bit.
B. Server Bundle.
C. Security Association Bundle.
D. Server Adjacency Bit.
ANSWER: C

132. An individual who is not authorized to use computer and who penetrates the system access controls to exploit a legitimate user's account is known as _____.
A. Misfeasor.
B. Malicious user.
C. Clandestine user.
D. Masquerader.
ANSWER: D

133. _____ detection involves the collection of data relating to the behavior of legitimate users over a period of time.
A. Rule based.
B. Integrity based.
C. Statistical anamoly.
D. All of the above.
ANSWER: C

134. PDA stands for _____.
A. personal digital assistant.

B. professional digital assistant.
C. personal data assistant.
D. professional data assistant.
ANSWER: A

135. Which of the following is not an field of audit record?
A. Subject.
B. Action.
C. Object.
D. Counter.
ANSWER: D

136. _____ is responsible for detecting errors and discarding any frames that contain errors.
A. Transport Layer.
B. MAC Layer.
C. Session Layer.
D. Network Layer.
ANSWER: B

137. PGP refers to _____.
A. People Good Policy.
B. Pretty Good Privacy.
C. Pretty Guarantee Policy.
D. Pretty Good Power.
ANSWER: B

138. In which phase is the virus idle?
A. Dormant phase.
B. Triggering phase.
C. Propogation phase.
D. Execution phase.
ANSWER: A

139. Which of the following virus made use of a Microsoft word macro embedded in an attachment?
A. Macro virus.
B. Melissa virus.
C. Encrypted virus.
D. Stealth virus.
ANSWER: B

140. The third generation uses which of the following antivirus software?
A. simple scanners.
B. heuristic scanners.
C. activity traps.
D. full-featured protection.
ANSWER: C

141. Which state of worm technology exploits against web servers?
A. Multiplatform.
B. Zero-day exploit.
C. Ultrafast spreading.

D. Multi-exploit.
ANSWER: D

142. State whether the following statement is true/false: The signature based worm is used to prevent worm scans from entering/leaving a network/host.
A. False.
B. Depends on the type of worm.
C. Unpredicatable.
D. True.
ANSWER: D

143. _____ encompasses three functional areas:authentication, confidentiality and Key management.
A. PGP.
B. .Kerberos
C. IPsec.
D. IEEE 802.11.
ANSWER: C

144. A Key concept that appears in both confidentiality and authentication mechanism of IPSec is _____.
A. Secure Audit.
B. Security Association.
C. Safety Association.
D. Secure Authentication.
ANSWER: B

145. In which of the following attack, the attacker is able to implant zombie software on a number of sites distributed throughout the internet.
A. Direct DDoS.
B. Indirect DDoS.
C. Reflector DDoS.
D. Traceback DDoS.
ANSWER: A

146. _____forms a barrier through which the traffic going in each direction must pass.
A. Firewall.
B. Virus.
C. Worm.
D. IPSec.
ANSWER: A

147. Which of the following is an example of circuit-level gateway?
A. SOCKS.
B. DNS.
C. UDP.
D. SMTP.
ANSWER: A

148. Which of the following statements is true? A. Each proxy is independent of other proxies on the basion host. B. Each proxy is configured to allow access to all host systems.
A. Both A and B.

B. Only A.
C. Neither A or B.
D. Only B.
ANSWER: B

149. _____ firewall is a software module used to secure an individual host.
A. Personal.
B. Transport.
C. Host-Based.
D. Presentation.
ANSWER: C

150. An important element of Intrusion preventions is _____.
A. Digital Signature.
B. Kerberos.
C. Warning.
D. Password Management.
ANSWER: D

Staff Name
Suguna M .