Department of Computer Science
Class: T.Y.B.Sc.(CS)
Semester: V
Subject: Information And Network Security
Sample Questions

Multiple Choice Questions

1)The principles of _____ ensures that only the sender and the intended recipients have access to the content of a message
a. Confidentiality
b. authentication
c. integrity
d. access control

2)In _____ attacks, there is no modification of message contents.
a. passive
b. active
c. active and passive
d. non active

3)If the recipient of a message has to be satisfied with the identity of the sender, the principle of _____ is observed
a. Confidentiality
b. authentication
c. integrity
d. access control

4)Allowing specific users specific access is termed as _____
a. Confidentiality
b. authentication
c. integrity
d. access control

5)The principle of _____ ensures that the sender of a message cannot later claim that the message was never sent.
a. access control
b. availability
c. authentication
d. non-repudiation

6)In _____ attack, the message contents are modified
a. passive
b. active
c. non active
d. non passive

7)Virus is a computer _____
a. file
b. program

c. database
d. network

8)A _____ replicates itself by creating its own copies, in order to bring the network to a halt.
a. virus
b. Worm
c. Trojan
d. bomb

9)The language that we commonly used can be termed as _____
a. plaint text
b. pair text
c. simple text
d. rough test

10)The codified language can be termed as _____
a. caeser text
b. cipher text
c. complex text
d. clear text

11)In substitution cipher, the following happens
a. characters are replaced by other characters
b. rows are replaced by characters
c. columns are replaced by rows
d. matrix is replaced by rows

12)Caesar cipher is an example of _____
a. substitution cipher
b. transposition cipher
c. substitution and transposition
d. cipher block test

13)Cryptanalysis is a person who _____
a. devices cryptography solutions
b. attempts to break cryptography solutions
c. attempts not to break cryptography solutions
d. devices non-cryptography solutions

14)Homophonic cipher is _____ type of cipher
a. substitution cipher
b. transposition cipher
c. substitution and transposition
d. cipher block test

15)Conversion of plain text into cipher text is called as _____
a. encryption
b. decryption
c. digital signature
d. data signature

16) Conversion of cipher text into plain text is called as _____
a. encryption
b. decryption
c. digital signature
d. data signature

17)The matrix theory is used in the _____ technique.
a. Hill cipher
b. Monoalphabetic cipher
c. playfair cipher
d. code cipher

18)In diffie-hellman Key exchange algorithm, the initial two numbers are called as _____ and _____
a. p,q
b. a,b
c. r,s
d. n,g

19)In _____ , one bit of plain text is encrypted at a time
a. block cipher
b. bit cipher
c. stream cipher
d. straight cipher

20)In _____, one block of plaint text is encrypted at a time.
a. block cipher
b. bit cipher
c. stream cipher
d. straight cipher

21)_____ works on block mode.
a. CFB
b. OFB
c. CCB
d. CBC

22)DES encrypts blocks of _____ bits.
a. 64
b. 32
c. 56
d. 128

23)In AES, the 16-byte key is expanded into _____
a. 176 bytes
b. 200 bytes
c. 78 bytes
d. 184 bytes

24)In IDEA, the key size is _____
a. 128 bytes
b. 256 bytes
c. 128bits
d. 256 bits

25)In asymmetric key cryptography, _____ keys are required per communicating party
a. 2
b. 3
c. 5
d. 4

26)_____ is a technique that facilitates hiding of a message which is to be kept secret inside another message.
a. substitution
b. transposition
c. steganography
d. criminology

27)An attack on cipher text message, where the attacker attempts to use all possible permutation and combination is called as _____
a. cipher attack
b. brute force attack
c. smurf attack
d. packet sniffing

28)In Cipher Block Chaining the initialization vector is used to maintain_____ for cipher text
a. simpler
b. unique
c. valuable
d. perfect

29)The private key _____
a. must be distributed
b. must remain secret with individual
c. must be shared with everyone
d. must be duplicated

30)If A and B want to communicate securely with each other, B must not know _____
a. A's private key
b. A's public key
c. B' private key
d. B's public key

31)if the sender encrypts the message with her private key, it achieves the purpose of _____
a. confidentiality
b. authentication
c. integrity

d. nonrepudation

32)A _____ is used to verify the integrity of the message.
a. Message Digest
b. Digital envelop
c. decryption
d. encryption

33)when two different message digest have the same value, it is called as _____
a. attack
b. hash
c. collision
d. cipher

34)_____ is a message digest algorithm
a. DES
b. IDEA
c. RSA
d. MD5

35)To verify the digital signature, we need the _____
a. sender's private key
a. sender's public key
a. receiver's private key
a. receiver's public key

36)A _____ can issue digital certificates.
a. CA
b. bank
c. shopkeeper
d. government

37)The CA with highest authority is called as _____ CA
a. main
b. master
c. manager
d. root

38)Firewall should be situated _____
a. inside a corporate network
b. outside a corporate network
c. anywhere
d. everywhere

39)A packet filter examines _____ packet
a. all
b. no
c. some
d. alternate

40)Application gateways are _____ than packet filters
a. less secure
b. more secure
c. equally secure
d. slowewer

41)Ipsec provides security at the _____ layer.
a. application
b. transport
c. network
d. data link

42)NAT stands for
a. natural account transfer
b. network account test
c. network address translation
d. network address transmission

43)Network address in the range 10)0)0)0 to 10)255)255)255 are called_____ addresses
a. public
b. private
c. protected
d. mac

44)_____ type of virus infects a master boot record and spreads when a system is booted from the disk containing the virus
a. Stealth virus
b. Polymorphic virus
c. Boot sector virus
d. Parasitic virus

45)_____ type of virus explicitly designed to hide itself from detection by antivirus software.
a. Stealth virus
b. Polymorphic virus
c. Boot sector virus
d. Parasitic virus

46)A _____ is a program that can replicate itself and send copies from computer to computer across network connections.
a. virus
b. Worm
c. Trojan
d. Bot

47)In _____ phase virus is activated to perform the function for which it was intended.
a. Dormant phase
b. propagation Phase

c. Triggering Phase
d. Execution phase

48)A _____ also known as trapdoor is a secret entry point into a program
a. backdoor
b. frontdoor
c. secretgate
d. privategate

49)_____ malicious program captures keystrokes on a compromised system
a. Kit
b. Keylogger
c. Flodders
d. zombie

50)_____ is set of hacker tool used after attacker has broken into a computer system and gained root-level access
a. zombie
b. Kit
c. Rootkit
d. exploits

51)The three classes of intruders are _____
a. Masquerader
b. Misfeasor
c. Cladestine users
d. sqad

52)password crackers report the following techniques for learning passwords are _____
a. Try user's phone number, room number etc.
b. Exhaustively try all short passwords
c. we can include inclusive
d. we can hack credentials

53)A system maintain a file that contains password for each authorized user This password file can be protect in _____ ways.
a. one-way function
b. Access control
c. two-way function
d. all-way function

54)_____ involves the collection of data relating to the behaviour of legitimate users over a period of time.
a. Statistical anomaly detection
b. Rule-based detection
c. Access control
d. Role- based detection

55)_____ approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
a. Threshold detection
b. Profile based
c. Anomaly detection
d. Penetration identification

56)_____ a profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.
a. Threshold detection
b. Profile based
c. Anomaly detection
d. Penetration identification

57)In _____ rules are developed to detect deviation from previous usage pattern
a. Threshold detection
b. Profile based
c. Anomaly detection
d. Penetration identification

58)_____ is an expert system approach that searches for suspicious behaviour.
a. Threshold detection
b. Profile based
c. Anomaly detection
d. Penetration identification

59)_____ involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder.
a. Statistical anomaly detection
b. Rule-based detection
c. Access control
d. Role- based detection

60)The fundamental tool for intrusion detection is the _____
a. Audit
b. Audit Record
c. subject
d. Action

61) Each audit record contains the following fields
a. subject
b. Action
c. audit name
d. reaction

62)For intrusion detection audit record contains various fields and_____ field contains receptors of action like programs, message records.
a. subject
b. Action
c. Object

d. Resource-Usage

63) For intrusion detection audit record contains various fields and_____ field defines unique time- and – date stamp identifying when the action took place.
a. Time-Stamp
b. Action
c. Object
d. Resource-Usage

64)Examples of metrics that are useful for profile –based intrusion detection is _____ which stores the record of the length of time between two related events.
a. Counter
b. Gauge
c. Interval timer
d. Resource utilization

65) Examples of metrics that are useful for profile –based intrusion detection are _____ which keeps the record of quantity of resources consumed during a specified period.
a. Counter
b. Gauge
c. Interval timer
d. Resource utilization

66)_____ technique to accelerate the spread of worm is to conduct a prior Internet scan to accumulate Internet addresses of vulnerable machines.
a. Multiplatform
b. Polymorphic
c. Metamorphic
d. Ultrafast spreading

67)_____ defines that newer worm are not limited to windows machine but can attack a variety of platforms.
a. Multiplatform
b. Polymorphic
c. Metamorphic
d. Ultrafast spreading

68)For virus detection _____ approach helps to identify the specific virus that has infected a program
a. Detection
b. Identification
c. Removal
d. specification

69) For virus detection _____ approach helps to remove all traces of the virus from infected program and restore it to its original state.
a. Detection
b. Identification
c. Removal

d. specification
70)_____ generation of antivirus software requires virus signature to identify a virus, which may contain wildcards.
a. first generation
b. Second generation
c. Third generation
d. Fourth generation

71)A Second generation scanner uses _____ rules to search for probable virus infection.
a. simple scanner
b. Heuristic scanners
c. Activity traps
d. Full featured protection

72)A second generation approach for antivirus software is integrity checking where _____ is appended to each program
a. file
b. password
c. Checksum
d. LRC

73)_____ generation of antivirus program are memory resident that identify a virus by its action rather than its structure in an infected program
a. first generation
b. Second generation
c. Third generation
d. Fourth generation

74)Behaviour blocking software helps in monitoring behaviour which includes following _____
a. Attempts to open, view, delete, and/or modify files
b. Attempts to format disk drives and other unrecoverable disk operation
c. Modification of critical system settings, like start-up settings
d. Attempts to delete and/or modify files

75)In _____ attack, an attacker is able to recruit a number of hosts throughout the internet to simultaneously or in a coordinated fashion launch an attack upon the target
a. DDOS
b. OSS
c. DSS
d. FOSS

76)In _____ attack the attacker takes control of multiple hosts over the Internet, instructing them to contact the target Web server
a. SYN flood attack
b. TCP attack
c. IP attack
d. unknown attack

77)In a _____ attack the attacker is able to implant zombie software on a number of sites distributed throughout the Internet
a. direct DDOS
b. reflector DDOS
c. TCP attack
d. ICMP attack

78)A _____ attack adds another layer of machines
a. direct DDOS
b. reflector DDOS
c. TCP attack
d. ICMP attack

79)A strategy for locating vulnerable machines, a process known as scanning is used. _____ scanning method uses information contained on an infected victim machine to find more host to scan
a. Random
b. Hit-list
c. Topological
d. Local subnet

80) A strategy for locating vulnerable machines, a process known as scanning is used. _____ scanning technique produces a high volume of Internet traffic, which may cause generalized disruption.
a. Random
b. Hit-list
c. Topological
d. Local subnet

81)The DDOS countermeasures defines
a. Attack prevention and pre-emption
b. Attack detection and filtering
c. Attack source traceback and identification
d. Attacks not detected.

82)_____ mechanisms enable the victim to endure attack attempts without denying service to legitimate clients.
a. Attack prevention and pre-emption
b. Attack detection and filtering
c. Attack source traceback and identification
d. Attacks not detected.

83)_____ is an attempt to identify the source of the attack is a first step in preventing future attacks.
a. Attack prevention and pre-emption
b. Attack detection and filtering
c. Attack source traceback and identification
d. Attacks not detected.

84)In Rotor machines each cylinder has ____ input and output pin.
a.25
b.26
c.32
d.64

85)The OSI security architecture focuses on _____
a. Security attack
b. Security Mechanism
c. Security service
d. Security Role

86)In connectionless transfer, provides assurance that the source of received data is as claimed is defined by _____ security service
a. Peer Entity Authentication
b. Data origin Authentication
c. Peer Entity & Data origin authentication
d. Peer Entity or Data origin authentication

87)_____ security service provides proof that the message was sent by the specified party
a. Nonrepudiation Origin
b. Nonrepudiation Destination
c. Nonrepudiation Origin and Nonrepudiation Destination
d. Peer Entity Authentication

88)_____ security mechanism defines the use of mathematical algorithm to transform data into a form that is readily intelligible
a. Digital signature
b. Access control
c. Data Integrity
d. Encipherment

89)The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts is known as __
a. Traffic padding
b. Access control
c. Data Integrity
d. Security label

90)The task involved in designing a particular security service are 1) The algorithm should be such that an opponent cannot defeat its purpose 2) Generate secret information to be used with algorithm
a. statement 1 is true and 2 is false
b. statement 2 is true and 1 is false
a. statement 1 and 2 are false
a. statement 1 and 2 are true

91)The symmetric cipher model contains _____ components
a.one

b. Four
c. Five
d. Six

92)In _____ type, the attacker knows about some pairs of plain text and corresponding cipher text for those pairs
a. Known plain text attack
b. Chosen plaint text attack
c. Cipher text only attack
d. Chosen text attack

93)In _____ attacker knows the cipher text, encryption algorithm, corresponding plain text block but attacker wants to discover the key used for encryption
a. Known plain text attack
b. Chosen cipher text attack
c. Cipher text only attack
d. Chosen text attack

94)The cipher text for Meet me by using Caesar cipher is _____
a. Phhw ph
b. oggy og
c. jbbq jb
d. nffu nf

95)Man in the middle attack is also called _____
a. bucket brigade attack
b. Woman in the middle attack
c. Chosen cipher text attack
d. Cipher text only attack

96)The XOR result of the operation 010101 and 010101 is ___
a.010101
b.000000
c.111111
d.101010

97)Double DES involves use of _____ keys
a. Two
b.one
c. Sixty-four
d. fifty-six

98)The attack which count the time required to decrypt the different blocks of cipher text
a. logic attack
b. timing attack
c. birthday attack
d. Scott attack

99)In _____ type of steganography technique selected letters of printed or typewritten text are overwritten in pencil
a. Character marking
b. Invisible ink
c. pin punctures
d. Typewriter correction ribbon

100)In _____ type of steganography technique small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light
a. Character marking
b. Invisible ink
c. pin punctures
d. Typewriter correction ribbon