
**PUNE VIDYARTHI GRIHA'S**
**COLLEGE OF SCIENCE AND TECHNOLOGY**
**Affiliated to University of Mumbai**

**Question Bank**

**Class: T.Y.B. Sc.CS** **Semester: V**
**Subject: Information and Network Security**

Unit I

1. In_____attacks, there is no modification of message contents.

a) Passive

b) Active

c) both of the above

d) Chiper attack

2. The principles of___ensures that only the sender and the intended recipients have access to the content of a message

   a) Confidential

   b) Authentication

   c) Access Control

   d) Integrity

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) Shift attack

d) Chipper attack

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) row and columns replace

12. caesar cipher is an example of _____

a) substitution cipher

b) transposition cipher

c) Stream cipher

d) Transsub cipher

13. What will be the cipher text of "hello there" using rail-fence technique.

a) olhel eehtr

b) elohl rhtee

c) elteh lohr

d) loleh hteer

14. Cryptanalysis is a person who _____

a) devices cryptography solutions

b) attempts to break cryptography solutions

c) attempt both

d) static

15. Homophonic cipher is_____type of cipher

a) substitution cipher

b) transposition cipher

c) a and b both
d) static cipher

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

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

18. The matrix theory is used in the_____ technique
a) Hill cipher
b) Monoalphabetic cipher
c) playfair cipher
d) code cipher

19. 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

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

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

22. _works on block mode.
a) CFB
b) OFB
c) CCB

d) CBC

23. DES encrypts blocks of_____bits.

a) 64

b) 32

c) 56

d) 128

24. In asymmetric key cryptography ,_____keys are required per communicating party

a) 2

b) 3

c) 5

d) 4

25. _____is a technique that facilitates hiding of a message which is to be kept secret inside other message.

a)substitution

b)transposition

c)steganography

d) chipper technology

26. all where the attack

attempts to use all possible

permutation and

combination is called as

a) cipher attack

b) brute force attack

c) smurf attack

d) packet sniffing

27. In Cipher Block Chaining the initialization vector is used to maintain _____for cipher text.

a)simpler

b)unique

c)valuable

d)perfect

28. The private key _____

a) must be distributed

b) must remain secret with individual

c) must be shared with everyone

d) must be duplicated

29. 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

30. if the sender encrypts the message with her private key, it achieves the purpose of ___

a)confidentiality

b)authentication

c)integrity

d)none of the above

31. A_____is used to verify the integrity of the message.

a)Message Digest

b)Digital envelop

c)decryption

d)encryption

32. when two different message digest have the same value, it is called as ____

a) attack

b)hash

c)collision

d)cipher

33. Vernam cipher is also called as

a. Reail- fence technique

b. One- time pad

c. Book cipher

d. Running-key cipher

34. What will be cipher text of the following "Network" using Caesar cipher key is 3

a. qhwzrun

b. ohysezn

c. bacghilm

d. opjklmw

35. cipher text for "Come home tomorrow" using columnar technique in

a. cmroermtoeowhmoo

b. eowoocmroerhmmto

c. metomocomehorrow

d. oermtocmreowhmoo

36. Cipher Text for HOW ARE YOU using a one time pad of NCBTZQARX

a) UQXTQUYFR

b) ABHJJKOPLO

c) TYOOVEFYO

d) VQPCRMEUY

37. _____is the Simplest mode of operation , where incoming plain text message is divided into block of 64 bit each

a) OFD

b) CTR

c) CFB

d) ECB

38. DES is also call as _____

a) DEA

b) AES

c) EAD

d) SAE

39. There are four importance algorithm modes

a) ECB,CBC,CFB,OFB
b) CBE,CBC,CFB,OBF
c) OFB,FBC,CBD,CFB
d) CBC,CFB,BFO,ERB

40. There are two type of algorithms

a) Stream and block cipher
b) Bit and Byte cipher
c) Cbc and cfb cipher
d) DES and AED

UNIT II

41. _____is a message digest algorithm

a)DES

b) IDEA

c)RSA

d)MD5

42. 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

43. A_____can issue digital certificates.

a)CA

b) bank

c)shopkeeper

d)government

44. The CA with highest authority is called as_____

a) main

b) master

c) cmanager

d) root

45. Firewall should be situated _____

a) inside a corporate network

b)outside a corporate network

c)anywhere

d)none of the above

38. .A packet filter examines_____packet

a)all

b)no c)some

d)alternate

39. Application gateways are_____than packet filters.

a)less secure

b) more secure

c) equally secure

d)slowewer

40. Ipsec provides security at the_____layer.

a)application

b)transport

c)network

d)data link

41. NAT stands for

a)natural account

transfer

b) network account test

c) network address translation

d) network address transmission

42. 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

46. _____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

47. _____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

48. .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

49. .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

49. A_____also known as trapdoor is a secret entry point into a program .

a)backdoor b)frontdoor

c)secretgate d)none of

the above

50. . _____malicious

program captures

keystrokes on a

compromised system.

a)Kit

b)Keylogger

c)Flodders

d)zombie

51. _____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

52. The three classes of intruders are _____

a)Masquerader

b)Misfeasor c)Cladestine

users d)All of the above

53. password crackers reports the following techniques for learning passwords are _____

a)Try user's hone number, room number etc. b)Exhaustively try all

short passwords

c) both 1 and 2

d) none of the above

54. .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) a and b both

d) none of the above

55. ___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

56. _____ 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

57. _____a profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

a)Threshold detection

b)Profile based

c)Anomaly detection

d)Penetration identification

58. In __rules are developed to detect deviation from previous usage pattern

a)Threshold detection

b)Profile based

c)Anomaly detection

d)Penetration identification

59. __is an expert system approach that searches for suspicious behavior.

a)Threshold detection

b)Profile based

c)Anomaly detection

d)Penetration identification

60. _____involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

a)Statistical anomaly detection

b)Rule-based detection c)Access

control

d)Role- based detection

61. The fundamental tool for intrusion detection is the _____

a) Audit

b) Audit Record

c)subject

d)Action

62. Each audit record contains the following

fields a)subject

b) Action

c) a and b both

d) none of the above

63. 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

64. 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

65. Examples of metrics that are useful for profile –based intrusion detection are___which stores the record of the length of time between two related events.

a)Counter b)Gauge

c)Interval timer

d)Resource utilization

66. 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

67. _technique to accelerate the spread of worm is to conduct a prior Internet scan to to accumulate Internet addresses of vulnerable machines.

a)Multiplatform

b)Polymorphic

c)Metamorphic d)Ultrafast

spreading

68. __defines that newer worms are not limited to windows machine but can attack a variety of platforms.

a)Multiplatform

b)Polymorphic

c)Metamorphic d)Ultrafast

spreading

69. For virus detection__approach helps to identify the specific virus that has infected a program

a)Detection

b)Identification

c)Removal

d)none of the above

70. For virus detection_approach helps to remove all traces of the virus from the infected program and restore it to its original state.

a)Detection

b)Identification

c)Removal

d)none of the above

## UNIT III

71. _____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

69. 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

70. A second generation approach for antivirus software is integrity checking where _____is appended to each program.

a)file

b)password

c)Checksum

d)LRC

71 . 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

72. Behavior blocking software helps in monitoring behavior 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)All of the above

73. In _____attack, an attacker is able to recruit a number of host throughout the internet to simultaneously or in a coordinated fashion launch an attack upon the target.

a)DDOS

b)OSS

C)DSS

D)FOSS

74. 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

75. 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)none of the above

76. A_____attack adds another layer of machines a)direct

DDOS

b)reflector DDOS

c)TCP attack

d)none of the above

77.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

78. 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

79. The DDOS countermeasures defines a)Attack

prevention and pre-emption

b) Attack detection and filtering

c) Attack source traceback and identification

d) All the above

80. _____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) All the above

81. _____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) All the above

82. In Rotor machines each cylinder has_ input and output pin. a)25

b)26

c)32

d)64

83. hhe OSI security architecture focuses on_____

a)Security attack

b) Security Mechanism

c) Security service

d) All of the above

84. 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) both a and b

d) none of the above

85. _____security service provides proof that the message was sent by the specified party.

a) Nonrepudiation Origin

b) Nonrepudiation Destination

c) both a and b

d) none of the above

86. _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

87. 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

88. 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 the secret information to be used with the 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

89. The symmetric cipher model contains_____components.

a)one

b) Four

c)Five

d)Six

90. 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

91. 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

92. The cipher text for Meet me by using Caesar cipher is _____

a) Phhw ph

b) oggy og

c) jbbq jb

d) nffu nf

93. an in the middle attack is also called _____.

a)bucket brigade attack

b) Woman in the middle attack

c) both a and b

d) none of the above

94. The XOR result of the operation 010101 and 010101 is ____

a)010101

b)000000

c)111111

d)101010

95. Double DES involves use of_____keys

a)Two

b)one c)Sixty

four

d)fifty six

96. 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) none of the above

97. In _____type of steganograhy 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

98. In_type of steganograhy 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

99. Determining the identity of a user is called

a) Authentication

b) authorization

c) confidentiality

d) access control

100. 2.is the most common authentication mechanism

a) Smart card

b) PIN

c) Biometrics

d) Password

101. Many organizations specify_____f or setting up rules re garding passwords

a) authentication law

b) password law

c) password policy

d) user id rule

102. forms the basis for the randomness of an authentication token.

a) I-factorb
b) 2-factor
c) 3-factor
d) 4-factor

103. In time-based tokens, the variable factor is

a) seed
b) random challenge
c) time
d) password

104. In_____authentication mechanism, only one party authenticates the other.

a) one-way
b) mutual
c) time-stamp-based
d) mutual with public keys

105. Biometric authentication works on the basis of

a) human characteristics
b) passwords
c) smart cards
d) PINs

106. Kerberos provides for

a) encryption
b) SSO
c) remote login

107. In certificate-based authentication, the user needs to enter a password for accessing

a) public-key file
b) private-key file
c) seed
d) Random

108. _____challenge are capable of crypto-graphic operations

a) Credit cards

b) ATM cards

c) Debit cards

d) Smart cards

109. To launch reflection attack, an attacker needs to open sessions

a) 2

b) 3

c) 4

d) 0 & 2

110. A packet filter examines _____packets.

a) all

b) no

c) some

d) alternate

111. adapts itself to the changing conditions.

b) Stateless static filter
c) Static packet filter
d) Adaptive packet filter

112. Application gateways are _____than packet filters

a) less secure

b) more secure

c) equally secure

d) slower

113. Indirect connections between the internal hosts and the packet filter are avoided.

a) Screened host firewall, Triple-homed bastion

b) Screened host firewall, Single-homed bastion

c) Screened host firewall, Null-homed bastion

d) Triple homed bastion

114. Application gateways are _____than packet filters.

a) less secure

b) more secure

c) equally secure

d) slower

115. _____allows reuse of IP addresses

a) Firewalls

b) IPSec

c) NAT

d) VPN

116. IPSec provides security at the _____Layer

a) Application

b) Transport

c) Network

d) data link

117. ISAKMP/Oakley is related to

a) SSL

b) SET

c) SHTTP

d) IPSec

118. Key management in IPSec is done by

a) tunnel mode
b) transport mode
c) IKE
d) ESP

.