CWIPEDIA.IN

Question Bank 1

1. Which of the following is an anti-virus program

A. Norton
B. K7
C. Quick heal
D. All Of These

D. All of these

2. All of the following are examples of real security and privacy threats except:

A. Hackers
B. Virus
C. Spam
D. Worm

C. Spam

Explanation : **Spam** or **SPAM** may refer to:

- Spamming, unsolicited or undesired electronic messages
- Email spam, unsolicited, undesired, or illegal email messages
- Messaging spam, spam targeting users of instant messaging (IM) services, sms or private messages within websites

3. Trojan horses are very similar to virus in the matter that they are computer programs that replicate copies of themselves

A. True
B. False

B. False

4. _____________ monitors user activity on internet and transmit that information in the background to someone else.

A. Malware
B. Spyware
C. Adware
D. None of these

B. Spyware

5. Viruses are __________.

A. Man Made
B. Naturally occur
C. Machine made
D. All of the above

A. Man made

6. Firewall is a type of ____________.

A. Virus
B. Security threat

C. Worm
D. None Of The Above

D. None of the above

Explanation : a **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules

7. Unsolicited commercial email is known as ____________.

A. Spam
B. Malware
C. Virus
D. Spyware

A. Spam

8. Which of the following is not an external threat to a computer or a computer network

A. Ignorance
B. Trojan horses
C. Adware
D. Crackers

A. Ignorance

9. When a person is harrassed repeatedly by being followed, called or be written to he / she is a target of

A. Bullying

B. Stalking
C. Identity theft
D. Phishing

B. Stalking

Explanation : **Stalking** is unwanted or repeated surveillance by an individual or group towards another person. Stalking behaviors are interrelated to harassment and intimidation and may include following the victim in person or monitoring them.

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.

10. Which of the following is a class of computer threat

A. Phishing
B. Soliciting
C. DoS Attacks
D. Stalking

C. DoS attacks

Explanation : **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

11. A lincense allows a user to use copyrighted material.

A. True
B. False

A. True

12. It is a program or hardware device that filters the information coming through an internet connection to a network or computer system.

A. Anti virus
B. Cookies
C. Firewall
D. Cyber safety

C. Firewall

13. It allow a visited website to store its own information about a user on the user’s computer.

A. Spam
B. Cookies
C. Malware
D. Adware

B. Cookies

14. It is stealing ideas or creations of others.

A. Plagiarism
B. Intellectual Property Rights
C. Piracy
D. All Of The Above

D. All of the above

15. Hacking a computer is always illegal and punishable by law.

A. *True*
B. False

A. True

16. Exploring appropriate and ethical behaviours related to online environments and digital media.

A. Cyber ethics
B. Cyber security
C. Cyber safety
D. Cyber law

A. Cyber ethics

17. Which of the following is digital certificate standard?

A. X.508
B. *X.509*
C. D.509
D. None of the Above

B. X.509

18. Which of the following technique is used to verify the integrity of the message?

A. *Message Digest*

B. Digital signature
C. Decryption algorithm
D. Protocol

A. Message digest

19. Which of the following principle is violated if computer system is not accessible?

A. Confidentiality
B. Availability
C. Access Control
D. Authentication

B. Availability

20. The certificate Authority signs the digital certificate with

A. User's public key
B. User's Private Key
C. It's own public key
D. It's Own Private Key

D. It's own Private key

21. Transit time and response time measure the _______ of a network

A. Performance
B. Reliability
C. Security
D. Longevity

A. Performance

22. The number of users on a network has the greatest impact on the network's ________

A. *Performance*
B. Reliability
C. Security
D. none of the above

A. Performance

23. Network failure is primarily a ________ issue.

A. Performance
B. *Reliability*
C. Security
D. none of the above

B. Reliability

24. ________ is a network reliability issue.

A. The number of users
B. The type of transmission medium
C. *The Frequency Of Failure*
D. Unauthorized access

C. The frequency of failure

25. ________ is a network reliability issue.

A. Catastrophe
B. The number of users
C. The type of transmission medium
D. Unauthorized access

A. Catastrophe

26. Unauthorized access is a network _______ issue.

A. Performance
B. Reliability
C. Security
D. none of the above

C. Security

27. A virus is a network _______ issue.

A. Performance
B. Reliability
C. Security
D. none of the above

C. Security

28. Encryption techniques improve a network's _______

A. Performance
B. Reliability
C. Security
D. Longevity

C. Security

29. A ________ is illicitly introduced code that damages a network device

A. Protocol
B. Virus
C. Catastrophe
D. Medium

B. Virus

30. Passwords are used to improve the ________ of a network.

A. Performance
B. Reliability
C. Security
D. Longevity

C. Security

31. Unauthorized access and viruses are issues dealing with network ________

A. Performance
B. Reliability
C. Security
D. none of the above

C. Security

32. Which of the following are network reliability issues?

A. frequency of failure

B. recovery time after a failure

C. catastrophe

D. All Of The Above

D. all of the above

33. When a hacker penetrates a network, this is a network ________ issue

A. Performance

B. Reliability

C. Security

D. none of the above

C. Security

34. When a server goes down, this is a network ________ issue.

A. Performance

B. Reliability

C. Security

D. none of the above

B. reliability

35. When an earthquake severs a fiber-optic cable, this is a network ________ issue

A. Performance

B. Reliability

C. Security

D. none of the above

A. Performance

36. When a network upgrades to a transmission medium with a data rate that is 100 times faster, this improves the _______ of the network.

A. *Performance*
B. Reliability
C. Security
D. none of the above

A. Performance

37. A company doubles the number of nodes on its network. The greatest impact will be on the _______ of the network

A. *Performance*
B. Reliability
C. Security
D. none of the above

A. Performance

38. A company changes its network configuration so that only one router instead of two can access the Internet. The greatest impact will be on the _______ of the network

A. Performance
B. Reliability
C. *Security*
D. None of the above

C. Security

39. A company requires its users to change passwords every month. This improves the _______ of the network

A. Performance
B. Reliability
C. Security
D. none of the above

C. Security

40. A company buys a computer to serve as a backup to its main server. This will mainly affect the _______ of the network.

A. Performance
B. Reliability
C. Security
D. none of the above

B. Reliability

41. A company requires each employee to power off his computer at the end of the day. This rule was implemented to make the network _______

A. perform better
B. more reliable
C. More Secure
D. more error-free

C. more secure

42. What Security tradeoff occurs while using IDS (Intrusion Detection System)?

A. Change in permission
B. Login Failures
C. Change in privilege
D. Performance Degradation

D. Performance degradation

Explanation : An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system

43. EDI (Electronic Data Interchange) use

A. requires an extranet
B. requires value added network
C. Can Be Done On Internet
D. requires a corporate intranet

C. can be done on internet

Explanation : EDI is a standardized method for transferring data between different computer systems or computer networks. It is commonly used for e-commerce purposes, such as sending orders to warehouses, tracking shipments, and creating invoices.

44. EDI (Electronic Data Interchange) over internet uses

A. MIME To Attach EDI Forms To E-Mail Messages
B. FTP to send business forms
C. HTTP to send business forms
D. SGML to send business forms

A. MIME to attach EDI forms to e-mail messages

45. For secure EDI (Electronic Data Interchange) transmission on internet

A. MIME is used
B. S/MIME Is Used
C. PGP is used
D. TCP/IP is used

B. S/MIME is used

46. EDI (Electronic Data Interchange) standard

A. is not easily available
B. Defines Several Hundred Transaction Sets For Various Business Forms
C. is not popular
D. defines only a transmission protocol

B. defines several hundred transaction sets for various business forms

47. By security in e-Commerce we mean

(i) Protecting an organization’s data resource from unauthorized access

(ii)Preventing disasters from happening

(iii) Authenticating messages received by an organization

(iv) Protecting messages sent on the internet from being read and understood by unauthorized persons/organizations

A. i, ii
B. ii, iii
C. iii, iv
D. I, Iii, Iv

D. i, iii, iv

48. A firewall is a

A. wall built to prevent fires from damaging a corporate intranet
B. security device deployed at the boundary of a company to prevent unauthorized physical access
C. Security Device Deployed At The Boundary Of A Corporate Intranet To Protect It From Unauthorized Access
D. device to prevent all accesses from the internet to the corporate intranet

C. security device deployed at the boundary of a corporate intranet to protect it from unauthorized access

49. A firewall may be implemented in

A. Routers Which Connect Intranet To Internet
B. bridges used in an intranet
C. expensive modem
D. user’s application programs

A. routers which connect intranet to internet

50. Firewall as part of a router program

A. filters only packets coming from internet
B. filters only packets going to internet
C. Filters Packets Travelling From And To The Intranet From The Internet
D. ensures rapid traffic of packets for speedy e-Commerce

C. filters packets travelling from and to the intranet from the internet

51. The Secure Electronic Transaction protocol is used for

A. Credit Card Payment
B. cheque payment
C. electronic cash payments
D. payment of small amounts for internet services

A. credit card payment

52. In SET protocol a customer encrypts credit card number using

A. his private key
B. Bank’s Public Key
C. bank’s private key
D. merchant’s public key

B. bank’s public key

53. In SET protocol a customer sends a purchase order

A. encrypted with his public key
B. in plain text form
C. encrypted using Bank’s public key
D. Using Digital Signature System

D. using digital Signature system

54. One of the problems with using SET protocol is

A. the merchant’s risk is high as he accepts encrypted credit card
B. the credit card company should check digital signature
C. The Bank Has To Keep A Database Of The Public Keys Of All Customers
D. the bank has to keep a database of digital signatures of all customers

C. the bank has to keep a database of the public keys of all customers

55. The bank has to have the public keys of all customers in SET protocol as it has to

A. Check The Digital Signature Of Customers
B. communicate with merchants
C. communicate with merchants credit card company
D. certify their keys

A. check the digital signature of customers

56. In electronic cheque payments developed, it is assumed that most of the transactions will be

A. customers to customers

B. customers to business
C. Business To Business
D. banks to banks

C. business to business

57. In cheque payment protocol, the purchase order form is signed by purchaser using

A. his public key
B. his private key
C. His Private Key Using His Signature Hardware
D. various public keys

C. his private key using his signature hardware

58. In the NetBill's protocol for small payments for services available in the internet

(i) the customer is charged only when the information is delivered

(ii)the vendor is guaranteed payment when information is delivered

(iii) the customer must have a certified credit card

(iv) the customer must have a valid public key

A. i, ii
B. i, ii, iii
C. i, ii, iii, iv
D. I, Ii, Iv

D. i, ii, iv

59. In NetBill's protocol for small payments for internet services

(i) Key to decrypt information is sent to customer by NetBill only when there is enough amount in debit account

(ii) The vendor supplies the key to NetBill server when he receives payment

(iii) Checksum of encrypted information received by customer is attached to his payment order

(iv) Vendor does not encrypt information purchased by customer

A. i, ii
B. I, Ii, Iii
C. i, ii, iii, iv
D. i, ii, iv

B. i, ii, iii

60. In Electronic cash payment

A. a debit card payment system is used
B. A Customer Buys Several Electronic Coins Which Are Digitally Signed By Coin Issuing Bank
C. a credit card payment system is used
D. RSA cryptography is used in the transactions

B. a customer buys several electronic coins which are digitally signed by coin issuing bank

61. Main function of proxy application gateway firewall is

A. to allow corporate users to use efficiently all internet services
B. To Allow Intranet Users To Securely Use Specified Internet Services
C. to allow corporate users to use all internet services
D. to prevent corporate users from using internet services

B. to allow intranet users to securely use specified internet services

62. Proxy application gateway

(i) acts on behalf of all intranet users wanting to access internet securely

(ii)monitors all accesses to internet and allows access to only specified IP addresses

(iii) disallows use of certain protocols with security problems

(iv) disallows all internet users from accessing intranet

A. i, ii
B. I, Ii, Iii
C. i, ii, iii, iv
D. ii, iii, iv

B. i, ii, iii

63. A hardened firewall host on an intranet

(i) has a proxy application gateway program running on it

(ii)Allows specified internet users to access specified services in the intranet

(iii) Initiates all internet activities requested by clients and monitors them

(iv) prevents outsiders from accessing IP addresses within the intranet

A. i, ii
B. i, ii, iii
C. I, Ii, Iii, Iv
D. ii, iii, iv

C. i, ii, iii, iv

64. A hardened firewall host on an Intranet is

A. a software which runs in any of the computers in the intranet
B. A Software Which Runs On A Special Reserved Computer On The Intranet
C. a stripped down computer connected to the intranet
D. a mainframe connected to the intranet to ensure security

B. a software which runs on a special reserved computer on the intranet

65. By encryption of a text we mean

A. compressing it
B. expanding it
C. Scrambling It To Preserve Its Security
D. hashing it

C. scrambling it to preserve its security

66. Encryption is required to

(i) protect business information from eavesdropping when it is transmitted on internet

(ii) efficiently use the bandwidth available in PSTN

(iii) to protect information stored in companies' databases from retrieval

(iv) to preserve secrecy of information stored in databases if an unauthorized person retrieves it

A. i and ii
B. ii and iii
C. iii and iv
D. I And Iv

D. i and iv

67. Encryption can be done

A. only on textual data
B. only on ASCII coded data
C. On Any Bit String
D. only on mnemonic data

C. on any bit string

68. By applying permutation (31254) and substitution by 5 characters away from current character (A Æ F , B Æ G etc..) the following string ABRACADABRA becomes

A. FGWCAAADRBF
B. RABCAAADRBF
C. WFGHFFFIWGF
D. None of the above

C. WFGHFFFIWGF

69. The following ciphertext was received. The plaintext was permuted using permutation (34152) and substitution. Substitute character by character +3 (A Æ D, etc). The plain text after decryption is: Cipher text :PDLJDLXHVQC

A. MAIGAIUESNZ
B. IAMAGENIUSZ
C. LDPDJHPLXVZ
D. IAMAGENIUSC

B. IAMAGENIUSZ

70. By symmetric key encryption we mean

A. *One Private Key Is Used For Both Encryption And Decryption*
B. private and public key used are symmetric
C. only public keys are used for encryption
D. only symmetric key is used for encryption

A. one private key is used for both encryption and decryption

71. The Acronym DES stands for

A. Digital Evaluation System
B. *Digital Encryption Standard*
C. Digital Encryption System
D. Double Encryption Standard

B. Digital Encryption Standard

72. DES works by using

A. *Permutation And Substitution On 64 Bit Blocks Of Plain Text*
B. only permutations on blocks of 128 bits
C. exclusive ORing key bits with 64 bit blocks
D. 4 rounds of substitution on 64 bit blocks with 56 bit keys

A. permutation and substitution on 64 bit blocks of plain text

73. DES

(i) is a symmetric key encryption method

(ii) guarantees absolute security

(iii) is implementable as hardware VLSI chip

(iv) is a public key encryption method

A. i and ii
B. ii and iii
C. I And Iii
D. iii and iv

C. i and iii

74. DES using 56 bit keys

A. Cannot be broken in reasonable time using presently available computers
B. Can be broken only if the algorithm is known using even slow computers.
C. Can Be Broken With Presently Available High Performance Computers.
D. It is impossible to break ever.

C. Can be broken with presently available high performance computers.

75. Triple DES uses

A. 168 bit keys on 64-bit blocks of plain text
B. Working On 64-Bit Blocks Of Plain Text And 56 Bit Keys By Applying DES Algorithm For Three Rounds.
C. Works with 144 bit blocks of plain text and applies DES algorithm once.
D. Uses 128 bit blocks of plain text and 112 bit keys and apply DES algorithm thrice.

B. Working on 64-bit blocks of plain text and 56 bit keys by applying DES algorithm for three rounds.

76. ripple DES

A. *Cannot Be Broken In Reasonable Time Using Presently Available Computers.*
B. Can be broken only if the algorithm is known using even slow computer.
C. Can be broken with presently available high performance computers.
D. It is impossible to break ever.

A. Cannot be broken in reasonable time using presently available computers.

77. Triple DES

A. is a symmetric key encryption method
B. *Guarantees Excellent Security*
C. is implementable as a hardware VLSI chip
D. is public key encryption method with three keys.

B. guarantees excellent security

78. Public key encryption method is a system

A. which uses a set of public keys one for each participant in e-Commerce
B. *In Which Each Person Who Wants To Communicate Has Two Keys; A Private Key Known To Him Only And A Public Key Which Is Publicized To Enable Others To Send Message To Him.*
C. which uses the RSA coding system.
D. which is a standard for use in e-Commerce.

B. in which each person who wants to communicate has two keys; a private key known to him only and a public key which is publicized to enable others to send message to him.

79. Public key system is useful because

A. it uses two keys.
B. There Is No Key Distribution Problem As Public Key Can Be Kept In A Commonly Accessible Database.
C. private key can be kept secret.
D. it is a symmetric key system.

B. there is no key distribution problem as public key can be kept in a commonly accessible database.

80. In public key encryption if A wants to send an encrypted message

A. A encrypts message using his private key
B. A encrypts message using B’s private key
C. A Encrypts Message Using B’s Public Key
D. A encrypts message using his public key

C. A encrypts message using B’s public key

81. In public key encryption system if A encrypts a message using his private key and sends it to B

A. If B Knows It Is From A He Can Decrypt It Using A’s Public Key
B. Even if B knows who sent the message it cannot be decrypted
C. It cannot be decrypted at all as no one knows A’s private key
D. A should send his public key with the message

A. if B knows it is from A he can decrypt it using A’s public key

82. Message can be sent more securely using DES by

A. encrypting plain text by a different randomly selected key for each transmission
B. Encrypting Plain Text By A Different Random Key For Each Message Transmission And Sending The Key To The Receiver Using A Public Key System
C. using an algorithm to implement DES instead of using hardware
D. designing DES with high security and not publicizing algorithm used by it

B. encrypting plain text by a different random key for each message transmission and sending the key to the receiver using a public key system

83. DES and public key algorithm are combined

(i) to speed up encrypted message transmission

(ii)to ensure higher security by using different key for each transmission

(iii) as a combination is always better than individual system

(iv) as it is required in e-Commerce

A. I And Ii
B. ii and iii
C. iii and iv
D. i and iv

A. i and ii

84. A digital signature is

A. a bit string giving identity of a correspondent

B. a unique identification of a sender
C. An Authentication Of An Electronic Record By Tying It Uniquely To A Key Only A Sender Knows
D. an encrypted signature of a sender

C. an authentication of an electronic record by tying it uniquely to a key only a sender knows

85. A digital signature is required

(i) to tie an electronic message to the sender's identity

(ii)for non repudiation of communication by a sender

(iii) to prove that a message was sent by the sender in a court of law

(iv) in all e-mail transactions

A. i and ii
B. I, Ii, Iii
C. i, ii, iii, iv
D. ii, iii, iv

B. i, ii, iii

86. A hashing function for digital signature

(i) must give a hashed message which is shorter than the original message

(ii)must be hardware implementable

(iii) two different messages should not give the same hashed message

(iv) is not essential for implementing digital signature

A. i and ii
B. ii and iii
C. I And Iii
D. iii and iv

C. i and iii

87. Hashed message is signed by a sender using

A. his public key
B. His Private Key
C. receiver’s public key
D. receiver’s private key

B. his private key

88. While sending a signed message, a sender

A. Sends Message Key Using Public Key Encryption Using DES And Hashed Message Using Public Key Encryption
B. sends message using public key encryption and hashed message using DES
C. sends both message and hashed message using DES
D. sends both message and hashed message using public key encryption

A. sends message key using public key encryption using DES and hashed message using public key encryption

89. The responsibility of a certification authority for digital signature is to authenticate the

A. hash function used
B. private keys of subscribers
C. Public Keys Of Subscribers

D. key used in DES

C. public keys of subscribers

90. Certification of Digital signature by an independent authority is needed because

A. it is safe
B. it gives confidence to a business
C. The Authority Checks And Assures Customers That The Public Key Indeed Belongs To The Business Which Claims Its Ownership
D. private key claimed by a sender may not be actually his

C. the authority checks and assures customers that the public key indeed belongs to the business which claims its ownership

91. What does IP mean?

A. Instance Principle
B. Internet Protocol
C. Instant Protocol
D. Intellectual Property

B. Internet Protocol

92. What happens to your data when it is encrypted?

A. It is transferred to a third party, encoded, then sent back.
B. It is compressed, renamed, and archived.

C. It is sent through a series of supercomputers to be compressed multiple times.
D. It Is Recorded To Retain Privacy From Third-Parties.

D. It is recorded to retain privacy from third-parties.

93. What is a computer virus?

A. A virus is the same as a cookie in that it is stored on your computer against your permission.
B. A virus is friendly software that is simply mislabeled.
C. Malicious software that merely stays dormant on your computer.
D. Malicious Software That Inserts Itself Into Other Programs.

D. Malicious software that inserts itself into other programs.

94. Which of the following is valid difference between a Virus and a Spyware ?

A. Spyware damages data and also steals sensitive private information
B. Virus Damages Data, Spyware Steals Sensitive Private Information
C. Spyware damages data, Virus steals sensitive private information
D. Virus damages data and also steals sensitive private information

B. Virus damages data, Spyware steals sensitive private information

95. How to avoid Man-in-the-middle attacks?

A. Accept every SSL certificate, even the broken ones
B. Use connections without SSL
C. Use HTTPS Connections And Verify The SSL Certificate

D. None of the above

C. Use HTTPS connections and verify the SSL certificate

96. What happens during the TCP attack; Denial of Service?

A. A virus is sent to disable their dos prompt.
B. Viruses are sent to their ISP to deny them tech support.
C. A worm is loaded onto the victim's computer to disable their keyboard.
D. Information Is Repeatedly Sent To The Victim To Consume Their System Resources, Causing Them To Shut Down.

D. Information is repeatedly sent to the victim to consume their system resources, causing them to shut down.

97. What is Internet Protocol Security?

A. Methods To Secure Internet Protocol (IP) Communication.
B. Ways to disconnect your router in an emergency
C. Methods to secure a disconnected computer.
D. Methods to secure your documents from physical breaches.

A. Methods to secure Internet Protocol (IP) communication.

98. Which of the following is a valid Cyber / Internet Security requirement?

A. Authentication
B. Integrity
C. Confidentiality
D. All Of The Given Options Are Correct

D. All of the given options are correct

99. Digital signatures provide which of the following ?

A. Authentication
B. Non-repudiation
C. Integrity protection
D. All Of The Given Options Are Correct

D. All of the given options are correct

100. In which of the following protocols does a website (if accessed using the protocol) encrypt the session with a Digital Certificate?

A. TCP
B. SHTTP
C. HTTPS
D. XHTTP

C. HTTPS