P.D.E.A's

Prof Ramkrishna More Arts, Commerce and Science College, Akurdi Pune-44

Introduction to Cyber Security

Practice MCQ Questions with Solutions

Module 1: Pre-requisites in Information and Network Security

Chapter-1: Overview of Networking Concepts

1. Physical or logical arrangement of network is
    a) Topology
    b) Routing
    c) Networking
    d) None of the mentioned

    Answer: a
2. In this topology there is a central controller or hub
    a) Star
    b) Mesh
    c) Ring
    d) Bus

    Answer: a
3. This topology requires multipoint connection
    a) Star
    b) Mesh
    c) Ring
    d) Bus

    Answer: d
4. Data communication system spanning states, countries, or the whole world is
    a) LAN
    b) WAN
    c) MAN
    d) None of the mentioned

    Answer: b
5. Data communication system within a building or campus is
    a) LAN
    b) WAN
    c) MAN
    d) None of the mentioned

    Answer: a

6. Expand WAN
    a) World area network
    b) Wide area network
    c) Web area network
    d) None of the mentioned
    Answer: b
7. What is the access point (AP) in wireless LAN?
    a) device that allows wireless devices to connect to a wired network
    b) wireless devices itself
    c) both (a) and (b)
    d) none of the mentioned
    Answer:a
8. In wireless ad-hoc network
    a) access point is not required
    b) access point is must
    c) nodes are not required
    d) none of the mentioned
    Answer:a
9. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?
    a) CDMA
    b) CSMA/CA
    c) ALOHA
    d) none of the mentioned
    Answer: b
10. In wireless distribution system
    a) multiple access point are inter-connected with each other
    b) there is no access point
    c) only one access point exists
    d) none of the mentioned
    Answer:a
11. A wireless network interface controller can work in
    a) Infrastructure mode
    b) ad-hoc mode
    c) both (a) and (b)
    d) none of the mentioned
    Answer:c

12. In wireless network an extended service set is a set of

a) Connected basic service sets

b) all stations

c) all access points

d) none of the mentioned

Answer:a

13. Mostly _____ is used in wireless LAN.

a) time division multiplexing

b) orthogonal frequency division multiplexing

c) space division multiplexing

d) none of the mentioned

Answer:b

14. Which one of the following event is not possible in wireless LAN.

a) Collision detection

b) Acknowledgement of data frames

c) multi-mode data transmission

d) none of the mentioned

Answer:a

15. What is Wired Equivalent Privacy (WEP) ?

a) security algorithm for ethernet

b) security algorithm for wireless networks

c) security algorithm for usb communication

d) none of the mentioned

Answer:b

16. What is WPA?

a) wi-fi protected access

b) wired protected access

c) wired process access

d) wi-fi process access

Answer:a

Chapter-2:Information Security Concepts

17. When information is read or copied by someone not authorized to do so, the result is known as _____
    a) loss of confidentiality b) loss of integrity
    c) loss of availability d) All of the above

    Answer is: - a
18. When information is modified in unexpected ways, the result is known as _____
    a) loss of confidentiality b) loss of integrity
    c) loss of availability d) All of the above

    Answer is: - b
19. When information can be erased or become inaccessible, the result is known as _____
    a)loss of confidentiality b) loss of integrity
    c) loss of availability d) None of the above

    Answer is: - c
20. When users cannot access the network or specific services provided on the network, they experience a _____
    a) Availability b) Denial of service
    c) diagnostic problem d) All of the above

    Answer is: - b
21. _____ is proving that a user is the person he or she claims to be.
    a)Authentication b) Authorization
    c) non-repudiation d) None of the above

    Answer is: - a
22. _____ is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.
    a)Authentication b) Authorization
    c) non-repudiation d) All of the above

    Answer is: - b
23. When the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity is known _____ .
    a)Authentication b) Authorization
    c) non-repudiation d) None of the above

    Answer is: - c

24. A _____ attack attempts to learn or make use of information from the system but does not affect system resources.
    a)active b) passive
    c) None of the above d) All of the above
    Answer is: - b
25. A _____ attack attempts modification of the data stream or the creation of a false stream.
    a)active b) passive
    c) None of the above d) All of the above
    Answer is: - a
26. _____ is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.
    a) E-commerce c) Computer Forensics
    b) None of the above d) All of the above

    Answer is: -c

Chapter-3:Security Threats and Vulnerabilities

27. What is the correct approach for addressing security and organization objectives?
    a. Security and organization objectives should be developed separately.
    b. Security should drive organization objectives.
    c. Security should support organization objectives.
    d. The site security officer should approve or reject organizationobjectives.

    Answer is:-c
28. A qualitative risk assessment is used to identify:
    a. Vulnerabilities, threats, and countermeasures
    b. Vulnerabilities, threats, threat probabilities, and countermeasures
    c. Assets, risks, and mitigation plans
    d. Vulnerabilities and countermeasures

    Answer is:-b
29. The impact of a specific threat is defined as:
    a. The cost of recovering the asset
    b. The cost required to protect the related asset
    c. The effect of the threat if it is realized
    d. The loss of revenue if it is realized

    Answer is:-c
30. The statement, “Information systems should be configured to requirestrong passwords,” is an example of a/an:
    a. Security requirement
    b. Security policy
    c. Security objective
    d. Security control

    Answer is:-b

31. An organization employs hundreds of office workers that use computers to perform their tasks. What is the best plan for informing employees about security issues?
    a. Include security policy in the employee handbook
    b. Perform security awareness training at the time of hire and annually thereafter

c.Perform security awareness training at the time of hire

    d. Require employees to sign the corporate security policy

Answer is:-b

32. An information system that processes sensitive information is configured to require a valid userid and strong password from any user. This process of accepting and validating this information is known as:
    a. Authentication
    b. Strong authentication
    c. Two-factor authentication
    d. Single sign-on

Answer is:-a

33. Palm scan, fingerprint scan, and iris scan are forms of:
    a. Strong authentication
    b. Two-factor authentication
    c. Biometric authentication
    d. Single sign-on

Answer is:-c

Chapter-4:Cryptography / Encryption

34. The method of hiding the secret is:
    (a) Cryptography (b) Steganography
    (c) Stenography (d) Cryptanalysis

Answer: a

35. In cryptography, what is cipher?
    a) algorithm for performing encryption and decryption
    b) encrypted message
    c) both (a) and (b)
    d) none of the mentioned

Answer: a

36. In asymmetric key cryptography, the private key is kept by
    a) sender b) receiver
    c) sender and receiver d) all the connected devices to the network

Answer:b

37. In cryptography, the order of the letters in a message is rearranged by

a) transpositional ciphers b) substitution ciphers

c) both (a) and (b) d) none of the mentioned

Answer:a

38. The _____is the original message before transformation.

A) ciphertext B) plaintext

C) secret-text D) none of the above

Answer:B

39. The _____ is the message after transformation.

A) ciphertext B) plaintext

C) secret-text D) none of the above

Answer:A

40. An _____ algorithm transforms ciphertext to plaintext.

A) encryption B) decryption

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

41. The _____ is a number or a set of numbers on which the cipher operates.

A) cipher B) secret

C)key D) none of the above

Answer:C

42. In an _____ cipher, the same key is used by both the sender and receiver.

A) symmetric-key B) asymmetric-key

C) either (a) or (b) D) neither (a) nor (b)

Answer:B

43. In an asymmetric-key cipher, the sender uses the_____ key.

A) private B) public

C) either (a) or (b) D) neither (a) nor (b)

Answer:B

44. In an asymmetric-key cipher, the receiver uses the _____ key.

A) private B) public

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

45. A _____ cipher replaces one character with another character.

A) substitution B) transposition

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

46. One commonly used public-key cryptography method is the _____ algorithm.

A) RSS B) RAS

C) RSA D) RAA

Answer:C

47. The Caesar cipher is a _____cipher that has a key of 3.

A) transposition B) additive

C) shift D) none of the above

Answer:C

48. The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.

A) transposition B) additive

C) shift D) none of the above

Answer:C

49. _____ ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.

A) Substitution B) Transposition

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

MCQ Question Bank on Cyber Law for Exams [100+ Objective Questions with Answers]

Cyber Law | Free Quizzes

LawBhoomi · July 23, 2022

(1) Tampering with Computer Source Documents is _____ offence.

(a) Bailable

(b) Non-bailable

(c) Non-cognizable

(d) Both (a) and (c)

(2) Every appeal to Cyber Appellate Tribunal shall be filed within a period of _____.

(a) 60 days

(b) 90 days

(c) 45 days

(d) 30 days

(3) Order passed by Controller is challengeable before :

(a) High Court

(b) Cyber Appellate Tribunal

(c) Adjudicatory Officer

(d) Supreme Court

(4) Child pornography is an offence under section _____.

(a) 67 C

(b) 67 A

(c) 67 B

(d) 67 D

(5) Section 66 A is striked down by the judiciary in the case of :

(a) Shreya Singhal v/s U.O.I.

(b) Syed Asifuddin v/s State of A.P.

(c) Ranjit Udeshi v/s State of Maharashtra

(d) Regina v/s Hicklin

(6) The authentication to be affected by use of asymmetric crypto system and hash function is knownas :

(a) Public key

(b) Private key

(c) Digital signature

(d) E-governance

(7) Which section of IT Act deals with the legal recognition of electronic records ?

(a) Section 4

(b) Section 2

(c) Section 5

(d) Section 6

(8) Which Section deals with cyber terrorism ?

(a) 66 C

(b) 66 B

(c) 66 D

(d) 66 F

(9) What is the maximum penalty for damage to computer, computer system ?

(a) Rs. 50 lakh

(b) Rs. 1 crore

(c) Rs. 5 crore

(d) 5 lakh

(10) What is the penalty for destroying computer source code ?

(a) Three yrs imprisonment or 5 lakh Rs. or both

(b) Three yrs imprisonment or 1 lakh Rs. or both

(c) Two yrs imprisonment or 2 lakh Rs. or both

(d) Three yrs imprisonment or 2 lakh penalty or both

(11) Amendment to IT Act 2000 came into effect on _____.

(a) 2008 Oct. 2

(b) 2009 July 3

(c) 2008 June 1

(d) 2009 Oct. 27

(12) Which are the Sections of IT Act that deal with credit card fraud ? (66c)

(a) 66, 66 C, 66 D

(b) 42, 67, 67 A, 67 B

(c) 43, 66, 66 C, 66 B

(d) None

(13) Which section of IT Act deals with the punishment for cheating by imprisonment by using computer resource ?

(a) Section 66 D

(b) Section 66 C

(c) Section 66 F

(d) Section 66 B

(14) Those who fail to furnish documents, return, report to the Controller of Certifying Authorities will be penalized upto :

(a) Rs. 5,000 per day

(b) Rs. 50,000

(c) Rs. 25,000 per day

(d) Rs. 1.5 lakh

(15) Licence to a Certifying Authority to issue electronic signature certificate will be valid for a period of :

(a) 5 yrs

(b) 10 yrs

(c) 2 yrs

(d) 7 yrs

(16) Cyber squatting is associated with :

(a) Domain Name Dispute

(b) IP addressing dispute

(c) e-mail dispute

(d) Password dispute

(17) The term ISP stands for :

(a) International Services Provider

(b) Internet Service Provider

(c) Internet Service Program

(d) Internet Social Policy

(18) Copying of a web-page or website and storing that copy for the purpose of speeding up subsequent access is called :

(a) Browsing

(b) File Swapping

(c) Caching

(d) Downloading

(19) The term EFT stands for :

(a) Emergency Fund Transfer

(b) Electric Fund Transfer

(c) Electronic Fund Transfer

(d) Electronic Fund Transmission

(20) Punishment for child pornography is provided under Section _____ of the I.T. Act.

(a) 66

(b) 67-A

(c) 67-B

(d) 67-C

(21) ICANN stands for :

(a) Internet Corporation for Assigned Names and Numbers

(b) International Commission for Assigned Names and Numbers

(c) International Corporation for Assisted Names and Numbers

(d) Internet Computer Assigned Names and Numbers

(22) The term computer is defined under Section _____ of the I.T. Act.

(a) 2(1) (a)

(b) 2(1) (t)

(c) 2(1) (i)

(d) 2(1) (h

(23) According to Section 78 of the IT Act, a _____ shall investigate any offence under the Act.

(a) Police Commissioner

(b) Police Constable

(c) Police Officer not below the rank of Inspector

(d) Deputy Superintendent of Police

(24) Sending of unsolicited bulk and commercial messages over the internet is _____.

(a) Stalking

(b) Phishing

(c) Spamming

(d) Spoofing

(25) Permitted use of disruptive activities or the threat thereof in cyber space is called _____.

(a) Commerce

(b) Credit Card fraud

(c) Net Banking

(d) Cyber Terrorism

(26) Information Technology Act was passed in the year _____.

(a) 1999

(b) 2000

(c) 2008

(d) 2012

(27) Computer virus is a _____.

(a) Programme

(b) File

(c) Disk

(d) Audio

(28) Repeated act of harassment after threatening behaviour is called as :

(a) Cyber stalking

(b) Data diddling

(c) Cyber theft

(d) Cryptography

(29) Salami attacks are used for the commission of _____.

(a) Financial crimes

(b) Personal crimes

(c) Property related crimes

(d) Physical crimes

(30) ACL stands for :

(a) Account Control List

(b) Air Conditioned List

(c) Access Control List

(d) Access Collection List

(31) IT Act 2000, amended in :

(a) 2005

(b) 2008

(c) 2011

(d) 2015

(32) Private key U/s 2(1) (ZC) is key of a secure key pair used to create a digital signature :

(a) Listed in the DSC issued to the subscriber by a Certifying Authority

(b) Not listed in the DSC issued to the subscriber by a Certifying Authority

(c) Sometime listed in DSC issued to the subscriber by Certifying Authority

(d) All of above

(33) As per IT Act, a subscriber may be :

(a) An individual

(b) Hindu undivided family applicant

(c) Company or firm

(d) All of above

(34) The DSC creates a “binding linkage” between :

(a) Controller and subscriber

(b) Subscriber and issuer

(c) Controller and Certifying Authority

(d) Police and Adjudicating Authority

(35) In the scheme of the Act, S. 43 to S. 45 are the ones that fall in the category of :

(a) Cyber crime

(b) Punishment provisions

(c) Cyber contraventions

(d) Only crimes

(36) Network service provider includes

(a) Originator

(b) Addressee

(c) Mobile Satellite Services

(d) None of above

(37) Cyberspace has :

(a) No national boundaries

(b) International jurisdiction

(c) Limited boundaries

(d) (a) and (b)

(38)Harassing someone through electronic message is offence of :

(a) Hacking

(b) Squatting

(c) Stalking

(d) Phishing

(39) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to :

(a) imprisonment for two years

(b) imprisonment upto three years

(c) imprisonment for six months

(d) imprisonment for life

(40) Against offence of cybers quatting victim is entitled to involve the provision :

(a) 411 of IPC

(b) 415 of IPC

(c) 268 of IPC

(d) 499 of IPC

(41) "Nigerian Scam 419" involve scam as :

(a) Phishing

(b) Cyber stalking

(c) Net extortion

(d) Pornography

(42) Information Technology Act, 2000 describes the offence of child pornography and prescribed punishment for it :

(a) Under Section 67

(b) Under Section 67 A

(c) Under Section 67 B

(d) Under Section 68

(43) _____ is a criminal offence of unlawfully obtaining money, property or services from a person, entity or institution, through coercion.

(a) Phishing

(b) Pornography

(c) Net or Cyber Extortion

(d) Credit Card Fraud

(44) _____ servers have chat rooms in which people from anywhere of the world can came

together and chat with each other.

(a) Channels

(b) Operators

(c) Internet Relay Chat

(d) Internet Protocol

(45) ICERT stands for :

(a) Indian Commercial and Economical

(b) Indian Commercial Emergency Response Team

(c) Indian Computer Emergency Response Team

(d) Indian Cyber Emergency Response Team

(46) ––––– Monitors all internet and other network activity, looking for suspicious data and preventing unauthorized access

(a) Firewall

(b) Intrusion detection system

(c) Data encryption

(d) None of the above

(47) Out of following which is the main authority is at the top and its main function is to issue licence to the certifying authority and to supervise his functions.

(a) Intermediator

(b) Controller of certifying authority

(c) subscriber

(d) None of the above.

(48) ––––––– means a system of a secure key pair consisting of a private key for creating digital signature and public key for verifying digital signature.

(a) Cryptography

(b) Asymmetric cryptosystem

(b) Symmetric cryptosystem

(d) None of the above

(49) ––––––– means a person who sends, generates, store or transmit any electronic massage.

(a) Intermediary

(b) Addressee

(c) Originator

(d) Controller.

(50) The receiving of unsolicited bulk emails is known as ––––––

(a) Virus

(b) Spoofing

(c) Spam

(d) Worms

(51) Out of the following which includes as an intermediary

(a) Online payment sites

(b) Internet service provide

(c) cyber café

(d) All the above

(52) Dot com job scam are cyber crimes included under ––––––.

(a) Social cyber crimes

(b) Economic cyber crimes

(c) cyber terrorism

(d) None of the above.

(53) Yahoo.inc Vs Akash Arora is a famaus case relating to ––––––.

(a) Cyber stalking

(b) Cyber squatting

(c) Cyber defamation

(d) None of the above

(54) The dispute resolution policy for domain name system comes from

(a) ICANN

(b) IANA

(c) ISOC

(d) IRTF

(55) WWW.amazon.com indicates that amazon is an ––––––.

(a) Education institute

(b) Government department

(c) Network provider

(d) Commercial organization.

(56) The value added network is used in ––––– form of communication.

(a) Electronic data interchange

(b) Electronic communication

(c) Cryptographic communication

(d) None of the above.

(57) ––––––– is not type of virus.

(a) Sparse infectors

(b) Stealth viruses

(c) Armoured viruses

(d) Metamorphic viruses

(58) Hash function are used for (encryption)

(a) Encryption

(b) Decryption

(c) Data integrity

(d) None of the above

(60) ––––– is the protected system used for identifying the person.

(a) Fire wall

(b) Biometrics

(c) Bothe (a) and (b)

(d) None of the above

(61) ISOC stands for –––––

(a) Internet socket

(b) Internal socket

(c) Internal society

(d) Internet society

(62) Information Technology Act was passed in the year _____.

(a) 1999

(b) 2000

(c) 2008

(d) 2012

(63) The science of sending secret cypher and decoding it, is called _____.

(a) Photography

(b) Cyprography

(c) Data diddling

(d) Cryptography

(64) Buying and selling of goods and services on the internet is called_____.

(a) E–Trade

(b) E–Commerce

(c) E–Challan

(d) E–Training

(65) Which Section of IT Act deals with the appointment of Controller of Certifying Authorities ?

(a) Section 17

(b) Section 15

(c) Section 10

(d) Section 5

(66) Which of the following Acts provides legal framework for e-governance in India ?

(a) IT (Amendment) Act, 2008

(b) Indian Penal Code

(c) IT Act, 2000

(d) None of the above

(67) Computer Virus is a :

(a) Programme

(b) Audio

(c) File

(d) Disk

(68) ACL stands for :

(a) Air Conditioned List

(b) Access Control List

(c) Access Collection List

(d) Account Control List

(69) Widely used security measure for blocking traffic in the network :

(a) fire window

(b) fire door

(c) fire wall

(d) fire exit

(70) Under Information Technology Act the purpose of digital signature is to :

(a) Forge the document

(b) Photocopy the document

(c) Digital Printing

(d) Authenticate the document

(71) Repeated act of harassment or threatening behaviour is called :

(a) Credit card fraud

(b) Cyber theft

(c) Cyber stalking

(d) Internet time theft

(72) Internet, protocol, addresses consist of four numbers from 0 to _____.

(a) 31

(b) 127

(c) 63

(d) 25

(73) Information Technology Act in based on model set of laws provided by :

(a) UNTCAD

(b) UNO

(c) UNCITRAL

(d) UNICEF

(74) Domain names are simply the _____ of the internet.

(a) Addresses

(b) Location

(c) Information

(d) Website

(75) What is an ISP ?

(a) Internet Service Provider

(b) Internet Sample Provider

(c) International Service Provider

(d) Internet Service Passenger

(76) A patent is an exclusive right granted by a _____ to the owner of an invention to make, use, manufacture.

(a) Country

(b) Government

(c) District

(d) World

(77) The Information Technology Act, 2000 was amended in the year _____.

(a) 2013

(b) 2012

(c) 2008

(d) 2011

(78) Computer means any device which performs :

(a) Logical functions

(b) Arithmetic functions

(c) Memory functions

(d) All of the above

(79) UNCITRAL relates to :

(a) Profession

(b) Business

(c) Trade

(d) Art

(80) The enactment of IT Act affected the provisions in :

(a) Transfer of Property Act

(b) Dowry Prohibition Act

(c) Indian Evidence Act

(d) Company law

(81) In Digital signature the key pair used is called :

(a) Public-personal

(b) Private-personal

(c) Personal-private

(d) Public-private

(82) ISO stands for :

(a) International Organization for Standardization

(b) International Service Organization

(c) International Security Organization

(d) International Secondary Organization

(83) The names with which companies exist in cyber world are called :

(a) Dangle names

(b) Device names

(c) Doodle names

(d) Domain names

(84) Hacking is prohibited under _____ of the IT Act, 2000.

(a) Sec. 64

(b) Sec. 65

(c) Sec. 66

(d) Sec. 63

(85) The IT Act, 2000 provides for the establishment of :

(a) Cyber Advisory Tribunal

(b) Computer Advisory Trust

(c) Cyber Appellate Tribunal

(d) Cyber Advisory Trust

(86) Cyber Crime is a crime in which computer is used as :

(a) Tool

(b) Target

(c) Both (a) and (b)

(d) None of the above

(87) Cyber Terrorism is an act injuring the :

(a) Sovereignty of India

(b) People of India

(c) Foreign relations

(d) All of the above

(88) Cyber Crime involves the theft of :

(a) Property

(b) Identity

(c) Money

(d) All of the above

(89) IP stands for :

(a) Internet procedure

(b) Internet position

(c) Internet protocol

(d) Internet program

(90) The cyber offence in which frauds are committed by inviting people to invest money and sharing financial information is :

(a) Hacking

(b) Squatting

(c) Piracy

(d) Fishing

91. Information Technology Act, 2000 is ACT NO. __ OF 2000?
(A)35
(B)21
(C)13
(D)1

92. Which among the following with regard to Information Technology Act, 2000 is NOT correct?
(A)It shall extend to the whole of India
(B)it does not apply to any offence or contravention thereunder committed outside India by any person
(C)it is an act to provide legal recognition for transactions carried out by means of electronic data
(D)It is the primary law in India dealing with cybercrime and electronic commerce

93. Information Technology Act, 2000 came into force on?
(A)1 January 2001
(B)11 June 2000
(C)17 October 2000
(D)24 December 2002

94. Who was the President of India who signed the Information Technology Act, 2000?
(A)A P J Abdul Kalam
(B)K R Narayanan
(C)Atal Bihari Vajpayee
(D)Pratibha Patil

95. "Digital signature" is defined under which section of IT Act,2000?
(A)Section 1
(B)Section 2

(C)Section 8
(D)Section 6

96. Information Technology Act, 2000 directed the formation of a Controller of Certifying Authorities to regulate the issuance of?
(A)Data license
(B)IP address in India
(C)digital signatures
(D)internet service provider license

97. Information Technology Act, 2000 amended which among the following to make them compliant with new technologies? i. Indian Penal Code, 1860 ii. Indian Evidence Act, 1872 iii. Banker's Book Evidence Act, 1891 iv. Reserve Bank of India Act, 1934
(A)i only
(B)i and iii only
(C)ii, iii and iv only
(D)All the above

98. A major amendment to Information Technology Act, 2000 was made in the year?
(A)2001
(B)2016
(C)2012
(D)2008

99. Which among the following was established under IT Act, 2000 to resolve disputes arising from the law?
(A)Cyber Appellate Tribunal
(B)Technology Disputes Bureau
(C)Cyber Administrative Tribunal
(D)IT Disputes Tribunal

100. Section 66A which penalized sending "offensive messages" was introduced in IT Act, 2000 through?
(A)Information Technology (Amendment) Act, 2008
(B)Information Technology (Amendment) Act, 2003
(C)Information Technology (Amendment) Act, 2015
(D)Information Technology (Amendment) Act, 2005

101. Which among the following is/are the major insertions in IT Act,2000 through Information Technology (Amendment) Act, 2008?

(A)Section 66A which penalized sending “offensive messages”

(B)Section 69, which gave authorities the power of “interception or monitoring or decryption of any information through any computer resource

(C)it introduced provisions addressing – pornography, child porn, cyber terrorism and voyeurism

(D)All the above

102. Which among the following offence under IT Act,2000 has the maximum penalty of imprisonment up to life?

(A)Using password of another person

(B)Securing access or attempting to secure access to a protected system

(C)Publication for fraudulent purpose

(D)Acts of cyberterrorism

103. Section 66A of IT Act,2000 has been struck down by Supreme Court’s Order dated 24th March, 2015 in which case?

(A)Shreya Singhal vs. Union of India

(B)Puttuswamy v. Union of India

(C)Shayara Bano vs Union Of India

(D)Indra Sawhney and Union of India

104. In the year 2020, Indian Government banned 59 Chinese mobile apps, including TikTok invoking which Section of IT Act, 2000?

(A)Section 66A

(B)Section 66F

(C)Section 72A

(D)Section 69A

105. The data privacy rules was introduced in IT Act, 2000 in the year?

(A)2008

(B)2011

(C)2015

(D)2020

(106) Child pornography is prohibited by _____ of IT Act, 2000.

(a) Sec. 64

(b) Sec. 65

(c) Sec. 66

(d) Sec. 67-B

References and Sources

https://bit.ly/3zqg1ay

https://bit.ly/3cBHBZb

⇧ SCROLL TO TOP

Cyber Security MCQ

This set of following multiple-choice questions and answers focuses on "Cyber Security". One shall practice these interview questions to improve their concepts for various interviews (campus interviews, walk-in interviews, and company interviews), placements, entrance exams, and other competitive exams.

1) In which of the following, a person is constantly followed/chased by another person or group of several peoples?

a. Phishing

b. Bulling

c. Stalking

d. Identity theft

Hide Answer | Workspace

Answer: c

Explanation: In general, Stalking refers to continuous surveillance on the target (or person) done by a group of people or by the individual person.

Cyber Stalking is a type of cybercrime in which a person (or victim) is being followed continuously by another person or group of several people through electronic means to harass the victim. We can also say that the primary goal of **Stalking** is to observe or monitor each victim's actions to get the essential information that can be further used for threatening, harassing, etc.

---

2) Which one of the following can be considered as the class of computer threats?

a. Dos Attack

b. Phishing

c. Soliciting

d. Both A and C

Hide Answer | Workspace

Answer: a

Explanation: A dos attack refers to the denial of service attack. It is a kind of cyber attack in which one tries to make a machine (or targeted application, website etc.) unavailable for its intended users. It is usually accomplished by disturbing the service temporarily or indefinitely of the target connected to the internet.

---

3) Which of the following is considered as the unsolicited commercial email?

a. Virus
b. Malware
c. Spam
d. All of the above

Hide Answer | Workspace

Answer: c

Explanation: It is a type of unsolicited email which is generally sent in bulk to an indiscriminate recipient list for commercial purpose. Generally, these types of mail are considered unwanted because most users don't want these emails at all.

---

4) Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

a. Malware
b. Spyware
c. Adware
d. All of the above

Hide Answer | Workspace

Answer: b

Explanation: It is generally defined as the software designed to enter the target's device or computer system, gather all information, observe all user activities, and send this information to a third party. Another important thing about the spyware is that it works in the background sends all information without your permission.

---

5) _____ is a type of software designed to help the user's computer detect viruses and avoid them.

a. Malware
b. Adware
c. Antivirus
d. Both B and C

Hide Answer | Workspace

Answer: c

Explanation: An antivirus is a kind of software that is specially designed to help the user's computer to detect the virus as well as to avoid the harmful effect of them. In some cases where the virus already resides in the user's computer, it can be easily removed by scanning the entire system with antivirus help.

---

6) Which one of the following is a type of antivirus program?

a. Quick heal
b. Mcafee
c. Kaspersky
d. All of the above

Hide Answer | Workspace

Answer: d

Explanation: Antivirus is a kind of software program that helps to detect and remove viruses form the user's computer and provides a safe environment for users to work on. There are several kinds of antivirus software are available in the market, such as Kaspersky, Mcafee, Quick Heal, Norton etc., so the correct answer is D.

---

7) It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_____:

a. Antivirus
b. Firewall

c. Cookies

d. Malware

Hide Answer | Workspace

Answer: b

Explanation: There are two types of firewalls - software programs and hardware-based firewalls. These types of firewalls filter each and every data packet coming from the outside environment such as network; internet so that any kind of virus would not be able to enter in the user's system. In some cases where the firewall detects any suspicious data packet, it immediately burns or terminates that data packet. In short, we can also say that it is the first line of defense of the system to avoid several kinds of viruses.

---

8) Which of the following refers to stealing one's idea or invention of others and use it for their own benefits?

a. Piracy

b. Plagiarism

c. Intellectual property rights

d. All of the above

Hide Answer | Workspace

Answer: d

Explanation: The stealing ideas or the invention of others and using them for their own profits can also be defined in several different ways, such as piracy, intellectual property rights, and plagiarism.

---

9) Read the following statement carefully and find out whether it is correct about the hacking or not?

It can be possible that in some cases, hacking a computer or network can be legal.

a. No, in any situation, hacking cannot be legal

b. It may be possible that in some cases, it can be referred to as a legal task

Hide Answer | Workspace

Answer: b

Explanation: Nowadays, hacking is not just referred to as an illegal task because there are some good types of hackers are also available, known as an ethical hacker. These types of hackers do not hack the system for their own purposes, but the organization hires them to hack their system to find security falls, loop wholes. Once they find the loop whole or venerability in the system, they get paid, and the organization removes that weak points.

---

10) Which of the following refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?

a. Cyber low
b. Cyberethics
c. Cybersecurity
d. Cybersafety

Hide Answer | Workspace

Answer: b

Explanation: Cyber Ethics refers to exploring the appropriate, ethical behaviors related to online environments and digital media.

---

11) Which of the following refers to the violation of the principle if a computer is no more accessible?

a. Access control
b. Confidentiality
c. Availability
d. All of the above

Hide Answer | Workspace

Answer: c

Explanation: Availability refers to the violation of principle, if the system is no more accessible.

---

12) Which one of the following refers to the technique used for verifying the integrity of the message?

a. Digital signature
b. Decryption algorithm
c. Protocol
d. Message Digest

Hide Answer | Workspace

Answer: d

Explanation: Message Digest is a type of cryptographic hash function that contains a string of digits that are created by the one-way hashing formula. It is also known as a type of technique used for verifying the integrity of the message, data or media, and to detect if any manipulations are made. Therefore the correct answer is D.

---

13) Which one of the following usually used in the process of Wi-Fi-hacking?

a. Aircrack-ng
b. Wireshark
c. Norton
d. All of the above

Hide Answer | Workspace

Answer: a

Explanation: The Aircrack-ng is a kind of software program available in the Linux-based operating systems such as Parrot, kali etc. it is usually used by users while hacking the Wi-Fi-networks or finding vulnerabilities in the network to capture or monitor the data packets traveling in the network.

---

14) Which of the following port and IP address scanner famous among the users?

a. Cain and Abel
b. Angry IP Scanner
c. Snort

d. Ettercap

Hide Answer | Workspace

Answer: b

Explanation: Angry IP Scanner is a type of hacking tool that is usually used by both white hat and black hat types of hackers. It is very famous among the users because it helps to find the weaknesses in the network devices.

---

15) In ethical hacking and cyber security, there are _____ types of scanning:

a. 1

b. 2

c. 3

d. 4

Hide Answer | Workspace

Answer: c

Explanation: There are usually three types of scanning in ethical hacking and cyber security. Therefore the correct answer is C.

---

16) Which of the following is not a type of scanning?

a. Xmas Tree Scan

b. Cloud scan

c. Null Scan

d. SYN Stealth

Hide Answer | Workspace

Answer: b

Explanation: Among the following-given options, the Cloud Scan is one, and only that is not a type of scanning.

17) In system hacking, which of the following is the most crucial activity?

a. Information gathering
b. Covering tracks
c. Cracking passwords
d. None of the above

Hide Answer | Workspace

Answer: c

Explanation: While trying to hack a system, the most important thing is cracking the passwords.

18) Which of the following are the types of scanning?

a. Network, vulnerability, and port scanning
b. Port, network, and services
c. Client, Server, and network
d. None of the above

Hide Answer | Workspace

Answer: a

Explanation: The vulnerability, port, and network scanning are three types of scanning.

19) Which one of the following is actually considered as the first computer virus?

a. Sasser
b. Blaster
c. Creeper
d. Both A and C

Hide Answer | Workspace

Answer: c

Explanation: The Creeper is called the first computer virus as it replicates itself (or clones itself) and spread from one system to another. It is created by Bob Thomas at BBN in early 1971 as an experimental computer program.

---

20) To protect the computer system against the hacker and different kind of viruses, one must always keep _____ on in the computer system.

a. Antivirus
b. Firewall
c. Vlc player
d. Script

Hide Answer | Workspace

Answer: b

Explanation: It is essential to always keep the firewall on in our computer system. It saves the computer system against hackers, viruses, and installing software form unknown sources. We can also consider it the first line of defense of the computer system.

---

21) Code Red is a type of _____

a. An Antivirus Program
b. A photo editing software
c. A computer virus
d. A video editing software

Hide Answer | Workspace

Answer: c

Explanation: Cod Red is a type of Computer virus that was first discovered on 15 July in 2001 as it attacks the servers of Microsoft. In a couple of next days, it infects almost 300,000 servers.

---

22) Which of the following can be considered as the elements of cyber security?

a. Application Security
b. Operational Security
c. Network Security
d. All of the above

Hide Answer | Workspace

Answer: d

Explanation: Application security, operational security, network security all are the main and unforgettable elements of Cyber Security. Therefore the correct answer is D.

---

23) Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system?

a. DDos and Derive-by Downloads
b. Malware & Malvertising
c. Phishing and Password attacks
d. All of the above

Hide Answer | Workspace

Answer: d

Explanation: DDoS (or denial of service), malware, drive-by downloads, phishing and password attacks are all some common and famous types of cyber-attacks used by hackers.

---

24) Which one of the following is also referred to as malicious software?

a. Maliciousware
b. Badware

c. Ilegalware

d. Malware

Hide Answer | Workspace

Answer: d

Explanation: Malware is a kind of short program used by the hacker to gain access to sensitive data/ information. It is used to denote many kinds of viruses, worms, Trojans, and several other harmful programs. Sometimes malware is also known as malicious software.

---

25) Hackers usually used the computer virus for _____ purpose.

a. To log, monitor each and every user's stroke

b. To gain access the sensitive information like user's Id and Passwords

c. To corrupt the user's data stored in the computer system

d. All of the above

Hide Answer | Workspace

Answer: d

Explanation: In general, hackers use computer viruses to perform several different tasks such as to corrupt the user's data stored in his system, to gain access the important information, to monitor or log each user's strokes. Therefore the correct answer is D.

---

26) In Wi-Fi Security, which of the following protocol is more used?

a. WPA

b. WPA2

c. WPS

d. Both A and C

Hide Answer | Workspace

Answer: b

Explanation: Nowadays, in Wi-Fi Security, the WPA2 is one of the most widely used protocols because it offers a more secure connection rather than the WPA. It is also known as the upgraded version of the WPA protocol.

---

27) The term "TCP/IP" stands for_____

a. Transmission Contribution protocol/ internet protocol
b. Transmission Control Protocol/ internet protocol
c. Transaction Control protocol/ internet protocol
d. Transmission Control Protocol/ internet protocol

Hide Answer | Workspace

Answer: b

Explanation: The term "TCP/IP" stood for Transmission Control Protocol/ internet protocol and was developed by the US government in the early days of the internet.

---

28) The response time and transit time is used to measure the _____ of a network.

a. Security
b. Longevity
c. Reliability
d. Performance

Hide Answer | Workspace

Answer: d

Explanation: On the basis of response time and transit time, the performance of a network is measured.

---

29) Which of the following factor of the network gets hugely impacted when the number of users exceeds the network's limit?

a. Reliability

b. Performance

c. Security

d. Longevity

Hide Answer | Workspace

Answer: d

Explanation: When the numbers of users on a network get increased and exceed the network's limit, therefore the performance is one of the factors of the network that is hugely impacted by it.

---

30) In the computer networks, the encryption techniques are primarily used for improving the _____

a. Security

b. Performance

c. Reliability

d. Longevity

Hide Answer | Workspace

Answer: a

Explanation: Encryption techniques are usually used to improve the security of the network. So the correct answer will be A.

---

31) Which of the following statements is correct about the firewall?

a. It is a device installed at the boundary of a company to prevent unauthorized physical access.

b. It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.

c. It is a kind of wall built to prevent files form damaging the corporate.

d. None of the above.

Hide Answer | Workspace

Answer: b

Explanation: A firewall can be the type of either a software or the hardware device that filters each and every data packet coming from the network, internet. It can also be considered as a device installed at the boundary of an incorporate to protect form unauthorized access. Sometimes firewall also refers to the first line of defense against viruses, unauthorized access, malicious software etc.

---

32) When was the first computer virus created?

a. 1970

b. 1971

c. 1972

d. 1969

Hide Answer | Workspace

Answer: b

Explanation: In 1970, the world's first computer virus was created by Robert (Bob) Thomas. This virus was designed as it creates copies of itself or clones itself and spreads one computer to another. So the correct answer will be 1970.

---

33) Which of the following is considered as the world's first antivirus program?

a. Creeper

b. Reaper

c. Tinkered

d. Ray Tomlinson

Hide Answer | Workspace

Answer: b

Explanation: Reaper is considered as the world's first antivirus program or software as it can detect the copies of a Creeper (the world's first man-made computer virus) and could delete it as well.

---

34) Which one of the following principles of cyber security refers that the security mechanism must be as small and simple as possible?

a. Open-Design
b. Economy of the Mechanism
c. Least privilege
d. Fail-safe Defaults

Hide Answer | Workspace

Answer: b

Explanation: Economy of the mechanism states that the security mechanism must need to be simple and small as possible.

---

35) Which of the following principle of cyber security restricts how privileges are initiated whenever any object or subject is created?

a. Least privilege
b. Open-Design
c. Fail-safe Defaults
d. None of the above

Hide Answer | Workspace

Answer: c

Explanation: The fail-safe Defaults principle of cyber security restricts how privileges are initiated whenever a subject or object is created. In cases where the privileges, rights, access or some other security-related attribute is not granted explicitly, it should also not granted access to the object.

---

36) Suppose an employee demands the root access to a UNIX system, where you are the administrator; that right or access should not be given to the employee unless that employee has work that requires certain rights, privileges. It can be considered as a perfect example of which principle of cyber security?

a. Least privileges
b. Open Design

c. Separation of Privileges

d. Both A & C

Hide Answer | Workspace

Answer: a

Explanation: The example given in the above question refers to the least privileges principle of cyber security. The least privileges principle of cyber security states that no rights, access to the system should be given to any of the employees of the organization unless he/she needs those particular rights, access in order to complete the given task. In short, we can say that its primary work is to restrict or control the assignment of rights to the employees.

---

37) Which of the following can also consider as the instances of Open Design?

a. CSS

b. DVD Player

c. Only A

d. Both A and B

Hide Answer | Workspace

Answer: d

Explanation: The Open Design is a kind of open design artifact whose documentation is publically available, which means anyone can use it, study, modify, distribute, and make the prototypes. However, the CSS (or Content Scrambling System) and DVD Player are both examples of open design.

---

38) Which one of the following principles states that sometimes it is become more desirable to rescored the details of intrusion that to adopt more efficient measure to avoid it?

a. Least common mechanism

b. Compromise recording

c. Psychological acceptability

d. Work factor

Hide Answer | Workspace

Answer: b

Explanation: The principle called compromise factor states that in some cases, it is more beneficial to records or document the details of the intrusion that to adopt more efficient measures to avoid it.

---

39) The web application like banking websites should ask its users to log-in again after some specific period of time, let say 30 min. It can be considered as an example of which cybersecurity principle?

a. Compromise recording
b. Psychological acceptability
c. Complete mediation
d. None of the above

Hide Answer | Workspace

Answer: c

Explanation: The complete mediation principle of cybersecurity requires that all the access must be checked to ensure that they are genuinely allowed. However, the example given in the above question can be considered as an example of Complete Mediation.

---

40) Which one of the following statements is correct about Email security in the network security methods?

a. One has to deploy hardware, software, and security procedures to lock those apps down.
b. One should know about what the normal behavior of a network look likes so that he/she can spot any changes, breaches in the behavior of the network.
c. Phishing is one of the most commonly used methods that are used by hackers to gain access to the network
d. All of the above

Hide Answer | Workspace

Answer: c

Explanation: In terms of Email Security, phishing is one of the standard methods that are used by Hackers to gain access to a network. The Email Security Tools can handle several types of attacks, such as the incoming attacks, and protect the outbound messages containing sensitive data/information as well.

---

41) Which of the following statements is true about the VPN in Network security?

a. It is a type of device that helps to ensure that communication between a device and a network is secure.
b. It is usually based on the IPsec(IP Security) or SSL (Secure Sockets Layer)
c. It typically creates a secure, encrypted virtual "tunnel" over the open internet
d. All of the above

Hide Answer | Workspace

Answer: d

Explanation: The term VPN stands for Virtual Private Network. It is a type of network security-enhancing tool that can be either a software program or a hardware device. It usually authenticates the communication between a device and a network by creating a secure encrypted virtual "tunnel". In general, the software VPNs are considered as the most cost-effective, user friendly over the hardware VPNs.

---

42) Which of the following type of text is transformed with the help of a cipher algorithm?

a. Transformed text
b. Complex text
c. Scalar text
d. Plain text

Hide Answer | Workspace

Answer: d

Explanation: The cipher algorithm is used to create an encrypted message by taking the input as understandable text or "plain text" and obtains unreadable or "cipher text" as output. It is usually used to protect the information while transferring one place to another place.

---

43) The term "CHAP" stands for _____

a. Circuit Hardware Authentication Protocols
b. Challenge Hardware Authentication Protocols
c. Challenge Handshake Authentication Protocols
d. Circuit Handshake Authentication Protocols

Hide Answer | Workspace

Answer: c

Explanation: The term "CHAP" stands for the Challenge Handshake Authentication Protocols. In computer networks, it can be defined as an authentication scheme that avoids the transfer of unencrypted passwords over the network. The "CHAP" is one of the many authentication schemes used by the Point To Point Protocol (PPP), which is a serial transmission protocol for wide networks Connections (WAN).

---

44) Which type of the following malware does not replicate or clone them self's through infection?

a. Rootkits
b. Trojans
c. Worms
d. Viruses

Hide Answer | Workspace

Answer: b

Explanation: The Trojans type of malware does not generate copies of them self's or clone them. The main reason why these types of viruses are referred to as the Trojans is the mythological story of the Greeks. In which some top-level accessions were hidden in the big wooden horse-like structure and given to the enemy as a gift. So that they can enter to the enemy's palace without come in any sight.

---

45) Which of the following malware's type allows the attacker to access the administrative controls and enables his/or her to do almost anything he wants to do with the infected computers.

a. RATs
b. Worms
c. Rootkits
d. Botnets

Hide Answer | Workspace

Answer: a

Explanation: The RAT is an abbreviation of Remote Access Trojans or Remote Administration Tools, which gives the total control of a Device, which means it, can control anything or do anything in the target device remotely. It allows the attacker administrative control just as if they have physical access to your device.

---

46) Which of the following statements is true about the Trojans?

a. Trojans perform tasks for which they are designed or programmed
b. Trojans replicates them self's or clone them self's through an infections
c. Trojans do nothing harmful to the user's computer systems
d. None of the above

Hide Answer | Workspace

Answer: a

Explanation: Trojans are a type of malware that will perform any types of actions for those they are design or programmed. Another important thing about Trojans is that the user may not know that the malware enters their system until the Trojan starts doing its job for which they

are programmed.

47) Which of the following is just opposite to the Open Design principle?

a. Security through obscurity
b. Least common mechanism
c. Least privileges
d. Work factor

Hide Answer | Workspace

Answer: a

Explanation: The "Security through obscurity" is an approach which just opposite to the Open Design principle. So the correct option is A.

48) Which of the following is a type of independent malicious program that never required any host program?

a. Trojan Horse
b. Worm
c. Trap Door
d. Virus

Hide Answer | Workspace

Answer: b

Explanation: Warm is a type of independent malicious program that does not require any host programs(or attached with some programs). They typically cause damages to the systems by consuming the bandwidths and overloading the servers. Warms are quite different from the virus as they are stand-alone programs, whereas viruses need some type of triggers to activate by their host or required human interaction.

49) Which of the following usually considered as the default port number of apache and several other web servers?

a. 20

b. 40

c. 80

d. 87

Hide Answer | Workspace

Answer: c

Explanation: The default port number used by the apache and several other web servers is 80. So the correct answer will be C.

---

50) DNS translates a Domain name into _____

a. Hex

b. Binary

c. IP

d. URL

Hide Answer | Workspace

Answer: d

Explanation: DNS stands for the Domain name system; the main work of a DNS is to translate the Domain name into an IP address that is understandable to the computers.

---

51) Which one of the following systems cannot be considered as an example of the operating systems?

a. Windows 8

b. Red Hat Linux

c. BSD Linux

d. Microsoft Office

Hide Answer | Workspace

Answer: d

Explanation: Microsoft office is a type of software used for creating and managing documents, which is one of the most famous products of the Microsoft organization. So the correct answer will be the D.

---

52) In the CIA Triad, which one of the following is not involved?

a. Availability
b. Confidentiality
c. Authenticity
d. Integrity

Hide Answer | Workspace

Answer: c

Explanation: CIA refers to Confidentiality, Integrity, and Availability that are also considered as the CIA triad. However, the CIA triad does not involve Authenticity.

---

53) In an any organization, company or firm the policies of information security come under_____

a. CIA Triad
b. Confidentiality
c. Authenticity
d. None of the above

Hide Answer | Workspace

Answer: a

Explanation: Confidentiality, Integrity, Availability are the three main principles. In Short, these three principles are also known as the CIA triad and plays a vital role as the cornerstone of the security structure of any organization.

---

54) Why are the factors like Confidentiality, Integrity, Availability, and Authenticity considered as the fundamentals?

a. They help in understanding the hacking process

b. These are the main elements for any security breach

c. They help to understand the security and its components in a better manner

d. All of the above

Hide Answer | Workspace

Answer: c

Explanation: Confidentiality, Integrity, Availability and Authenticity all these four elements helps in understanding security and its components.

---

55) In order to ensure the security of the data/ information, we need to _____ the data:

a. Encrypt

b. Decrypt

c. Delete

d. None of the above

Hide Answer | Workspace

Answer: a

Explanation: Data encryption is a type of method in which the plain text is converted into ciphertext, and only the authorized users can decrypt it back to plain text by using the right key. This preserves the Confidentiality of the Data.

---

56) Which one of the following is considered as the most secure Linux operating system that also provides anonymity and the incognito option for securing the user's information?

a. Ubuntu

b. Tails

c. Fedora

d. All of the above

Hide Answer | Workspace

Answer: b

Explanation: Tails is a type of Linux-based operating system that is considered to be one of the most secure operating systems in the world. It also provides many features such as anonymity and incognito options to insure that user information is always protected. The main reason why the tails operating system is famous among the user is that it is almost untraceable, which keep your privacy secure.

---

57) Which type following UNIX account provides all types of privileges and rights which one can perform administrative functions?

a. Client
b. Guest
c. Root
d. Administrative

Hide Answer | Workspace

Answer: d

Explanation: If a user uses the Root account of the UNIX operating system, he can carry out all types of administrative functions because it provides all necessary privileges and rights to a user.

---

58) Which of the following is considered as the first hacker's conference?

a. OSCON
b. DEVON
c. DEFCON
d. SECTION

Hide Answer | Workspace

Answer: c

Explanation: DEFCON is one of the most popular and largest Hacker's as well as the security consultant's conference. It is always held once a year in Las Vegas, Nevada, where hackers of all types (such as black hats, gray hats, and white hat hackers), government agents as well as security professionals from around the world attend the conference attends this meeting.

---

59) Which of the following known as the oldest phone hacking techniques used by hackers to make free calls?

a. Phreaking
b. Phishing
c. Cracking
d. Spraining

Hide Answer | Workspace

Answer: a

Explanation: Phreaking is considered as one of the oldest phone hacking techniques used by hackers to make free calls.

---

60) Name of the Hacker who breaks the SIPRNET system?

a. John Draper
b. Kevin Mitnick
c. John von Neumann
d. Kevin Poulsen

Hide Answer | Workspace

Answer: d

Explanation: The SIPRNET (or Advanced Research Project Agency Network) system was first hacked by Kevin Poulsen as he breaks into the Pentagon network.

For Videos Join Our Youtube Channel: Join Now

Feedback

- Send your Feedback to feedback@javatpoint.com

Help Others, Please Share

Learn Latest Tutorials

Splunk | SPSS | Swagger | Transact-SQL

Tumblr | ReactJS | Regex | Reinforcement Learning

R Programming

RxJS

React Native

Python Design Patterns

Python Pillow

Python Turtle

Keras

Preparation

Aptitude

Logical Reasoning

Reasoning

Verbal Ability

Interview Questions

Company Interview Questions

Trending Technologies

Artificial Intelligence

AWS Tutorial

AWS

Selenium tutorial

Selenium

Cloud Computing

Hadoop tutorial

Hadoop

ReactJS Tutorial

ReactJS

Data Science Tutorial

Data Science

Angular 7 Tutorial

Angular 7

Blockchain Tutorial

Blockchain

Git Tutorial

Git

Machine Learning Tutorial

Machine Learning

DevOps Tutorial

DevOps

B.Tech / MCA

DBMS tutorial
DBMS

Data Structures tutorial
Data Structures

DAA tutorial
DAA

Operating System
Operating System

Computer Network tutorial
Computer Network

Compiler Design tutorial
Compiler Design

Computer Organization and Architecture
Computer Organization

Discrete Mathematics Tutorial
Discrete Mathematics

Ethical Hacking
Ethical Hacking

Computer Graphics Tutorial
Computer Graphics

Software Engineering
Software Engineering

html tutorial
Web Technology

Cyber Security tutorial
Cyber Security

Automata Tutorial
Automata

C Language tutorial
C Programming

C++ tutorial
C++

Java tutorial
Java

.Net Framework tutorial
.Net

Python tutorial
Python

List of Programs
Programs

Control Systems tutorial
Control System

Data Mining Tutorial
Data Mining

Data Warehouse Tutorial
Data Warehouse