



ISC2

Exam Questions CISSP-ISSAP

Information Systems Security Architecture Professional

NEW QUESTION 1

Which of the following elements of planning gap measures the gap between the total potential for the market and the actual current usage by all the consumers in the market?

- A. Project gap
- B. Product gap
- C. Competitive gap
- D. Usage gap

Answer: D

NEW QUESTION 2

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

- A. PGP
- B. PTP
- C. IPSec
- D. NTFS

Answer: A

NEW QUESTION 3

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

- A. Policy Access Control
- B. Mandatory Access Control
- C. Discretionary Access Control
- D. Role-Based Access Control

Answer: D

NEW QUESTION 4

A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

- A. Denial-of-Service attack
- B. Vulnerability attack
- C. Social Engineering attack
- D. Impersonation attack

Answer: A

NEW QUESTION 5

You are the Security Consultant advising a company on security methods. This is a highly secure location that deals with sensitive national defense related data. They are very concerned about physical security as they had a breach last month. In that breach an individual had simply grabbed a laptop and ran out of the building. Which one of the following would have been most effective in preventing this?

- A. Not using laptop
- B. Keeping all doors locked with a guar
- C. Using a man-tra
- D. A sign in lo

Answer: C

NEW QUESTION 6

You want to implement a network topology that provides the best balance for regional topologies in terms of the number of virtual circuits, redundancy, and performance while establishing a WAN network. Which of the following network topologies will you use to accomplish the task?

- A. Bus topology
- B. Fully meshed topology
- C. Star topology
- D. Partially meshed topology

Answer: D

NEW QUESTION 7

Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two-factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or identifying pin number. Adam decides to implement smart cards but they are not cost effective. Which of the following types of hardware devices will Adam use to implement two-factor authentication?

- A. Biometric device
- B. One Time Password
- C. Proximity cards
- D. Security token

Answer: D

NEW QUESTION 8

Maria works as a Network Security Officer for Gentech Inc. She wants to encrypt her network traffic. The specific requirement for the encryption algorithm is that it must be a symmetric key block cipher. Which of the following techniques will she use to fulfill this requirement?

- A. IDEA
- B. PGP
- C. DES
- D. AES

Answer: C

NEW QUESTION 9

Which of the following protocols uses public-key cryptography to authenticate the remote computer?

- A. SSH
- B. Telnet
- C. SCP
- D. SSL

Answer: A

NEW QUESTION 10

Which of the following are the examples of technical controls? Each correct answer represents a complete solution. Choose three.

- A. Auditing
- B. Network architecture
- C. System access
- D. Data backups

Answer: ABC

NEW QUESTION 10

Which of the following tenets does the CIA triad provide for which security practices are measured? Each correct answer represents a part of the solution. Choose all that apply.

- A. Integrity
- B. Accountability
- C. Availability
- D. Confidentiality

Answer: ACD

NEW QUESTION 11

Which of the following attacks can be overcome by applying cryptography?

- A. Web ripping
- B. DoS
- C. Sniffing
- D. Buffer overflow

Answer: C

NEW QUESTION 16

Which of the following authentication methods prevents unauthorized execution of code on remote systems?

- A. TACACS
- B. S-RPC
- C. RADIUS
- D. CHAP

Answer: B

NEW QUESTION 17

The simplest form of a firewall is a packet filtering firewall. Typically a router works as a packet- filtering firewall and has the capability to filter on some of the contents of packets. On which of the following layers of the OSI reference model do these routers filter information? Each correct answer represents a complete solution. Choose all that apply.

- A. Transport layer
- B. Physical layer
- C. Data Link layer
- D. Network layer

Answer: AD

NEW QUESTION 20

Which of the following electrical events shows a sudden drop of power source that can cause a wide variety of problems on a PC or a network?

- A. Blackout
- B. Power spike
- C. Power sag
- D. Power surge

Answer: A

NEW QUESTION 22

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

- A. Containment
- B. Preparation
- C. Recovery
- D. Identification

Answer: A

NEW QUESTION 24

You work as a Network Administrator for NetTech Inc. You want to have secure communication on the company's intranet. You decide to use public key and private key pairs. What will you implement to accomplish this?

- A. Microsoft Internet Information Server (IIS)
- B. VPN
- C. FTP server
- D. Certificate server

Answer: D

NEW QUESTION 25

Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

- A. Risk analysis
- B. OODA loop
- C. Cryptography
- D. Firewall security

Answer: C

NEW QUESTION 29

Which of the following types of halon is found in portable extinguishers and is stored as a liquid?

- A. Halon-f
- B. Halon 1301
- C. Halon 11
- D. Halon 1211

Answer: D

NEW QUESTION 31

Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the disaster recovery plan?

- A. Structured walk-through test
- B. Simulation test
- C. Full-interruption test
- D. Parallel test

Answer: C

NEW QUESTION 34

In which of the following network topologies does the data travel around a loop in a single direction and pass through each device?

- A. Ring topology
- B. Tree topology
- C. Star topology
- D. Mesh topology

Answer: A

NEW QUESTION 36

You are the Network Administrator for a small business. You need a widely used, but highly secure hashing algorithm. Which of the following should you choose?

- A. AES
- B. SHA
- C. EAP
- D. CRC32

Answer: B

NEW QUESTION 41

Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead-space?

- A. Man trap
- B. Biometric device
- C. Host Intrusion Detection System (HIDS)
- D. Network Intrusion Detection System (NIDS)

Answer: A

NEW QUESTION 45

Which of the following refers to a location away from the computer center where document copies and backup media are kept?

- A. Storage Area network
- B. Off-site storage
- C. On-site storage
- D. Network attached storage

Answer: B

NEW QUESTION 50

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

- A. Email spoofing
- B. Social engineering
- C. Web ripping
- D. Steganography

Answer: D

NEW QUESTION 52

You work as a technician for Trade Well Inc. The company is in the business of share trading. To enhance security, the company wants users to provide a third key (apart from ID and password) to access the company's Web site. Which of the following technologies will you implement to accomplish the task?

- A. Smart cards
- B. Key fobs
- C. VPN
- D. Biometrics

Answer: B

NEW QUESTION 56

Which of the following layers of the OSI model corresponds to the Host-to-Host layer of the TCP/IP model?

- A. The transport layer
- B. The presentation layer
- C. The session layer
- D. The application layer

Answer: A

NEW QUESTION 58

Which of the following is an electrical event shows that there is enough power on the grid to prevent from a total power loss but there is no enough power to meet the current electrical demand?

- A. Power Surge
- B. Power Spike
- C. Blackout
- D. Brownout

Answer: D

NEW QUESTION 59

The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

- A. Disaster recovery planning
- B. SOA value proposition
- C. Software assets reuse
- D. Architectural components abstraction
- E. Business traceability

Answer: BCDE

NEW QUESTION 62

In your office, you are building a new wireless network that contains Windows 2003 servers. To establish a network for secure communication, you have to implement IPSec security policy on the servers. What authentication methods can you use for this implementation? Each correct answer represents a complete solution. Choose all that apply.

- A. Public-key cryptography
- B. Kerberos
- C. Preshared keys
- D. Digital certificates

Answer: BCD

NEW QUESTION 65

Which of the following two components does Kerberos Key Distribution Center (KDC) consist of? Each correct answer represents a complete solution. Choose two.

- A. Data service
- B. Ticket-granting service
- C. Account service
- D. Authentication service

Answer: BD

NEW QUESTION 70

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

- A. Service-oriented architecture
- B. Sherwood Applied Business Security Architecture
- C. Service-oriented modeling framework
- D. Service-oriented modeling and architecture

Answer: B

NEW QUESTION 71

Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

- A. Buffer-overflow attack
- B. Man-in-the-middle attack
- C. Shoulder surfing attack
- D. Denial-of-Service (DoS) attack

Answer: C

NEW QUESTION 73

A digital signature is a type of public key cryptography. Which of the following statements are true about digital signatures? Each correct answer represents a complete solution. Choose all that apply.

- A. In order to digitally sign an electronic record, a person must use his/her public key
- B. In order to verify a digital signature, the signer's private key must be use
- C. In order to digitally sign an electronic record, a person must use his/her private key
- D. In order to verify a digital signature, the signer's public key must be use

Answer: CD

NEW QUESTION 75

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

- A. Mutual
- B. Anonymous
- C. Multi-factor
- D. Biometrics

Answer: C

NEW QUESTION 79

You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

- A. Eradication
- B. Identification
- C. Recovery
- D. Containment

Answer: A

NEW QUESTION 82

Which of the following processes is used to identify relationships between mission critical applications, processes, and operations and all supporting elements?

- A. Critical path analysis
- B. Functional analysis
- C. Risk analysis
- D. Business impact analysis

Answer: A

NEW QUESTION 85

Which of the following devices is a least expensive power protection device for filtering the electrical stream to control power surges, noise, power sags, and power spikes?

- A. Line Conditioner
- B. Surge Suppressor
- C. Uninterrupted Power Supply (UPS)
- D. Expansion Bus

Answer: C

NEW QUESTION 88

You work as a Network Administrator for Blue Bell Inc. The company has a TCP-based network. The company has two offices in different cities. The company wants to connect the two offices by using a public network. You decide to configure a virtual private network (VPN) between the offices. Which of the following protocols is used by VPN for tunneling?

- A. L2TP
- B. HTTPS
- C. SSL
- D. IPSec

Answer: A

NEW QUESTION 90

John works as a Network Administrator for NetPerfect Inc. The company has a Windows-based network. John has been assigned a project to build a network for the sales department of the company. It is important for the LAN to continue working even if there is a break in the cabling. Which of the following topologies should John use to accomplish the task?

- A. Star
- B. Mesh
- C. Bus
- D. Ring

Answer: B

NEW QUESTION 94

Which of the following encryption algorithms are based on block ciphers?

- A. RC4
- B. Twofish
- C. Rijndael
- D. RC5

Answer: BCD

NEW QUESTION 99

The OSI model is the most common networking model used in the industry. Applications, network functions, and protocols are typically referenced using one or more of the seven OSI layers. Of the following, choose the two best statements that describe the OSI layer functions. Each correct answer represents a complete solution. Choose two.

- A. Layers 1 and 2 deal with application functionality and data formattin
- B. These layers reside at the top of the mode

- C. Layers 4 through 7 define the functionality of IP Addressing, Physical Standards, and Data Link protocol
- D. Layers 5, 6, and 7 focus on the Network Application, which includes data formatting and session contro
- E. Layers 1, 2, 3, and 4 deal with physical connectivity, encapsulation, IP Addressing, and Error Recover
- F. These layers define the end-to-end functions of data deliver

Answer: CD

NEW QUESTION 103

Which of the following is the technology of indoor or automotive environmental comfort?

- A. HIPS
- B. HVAC
- C. NIPS
- D. CCTV

Answer: B

NEW QUESTION 104

Which of the following protocols provides certificate-based authentication for virtual private networks (VPNs)?

- A. PPTP
- B. SMTP
- C. HTTPS
- D. L2TP

Answer: D

NEW QUESTION 109

Which of the following security protocols provides confidentiality, integrity, and authentication of network traffic with end-to-end and intermediate-hop security?

- A. IPSec
- B. SET
- C. SWIPE
- D. SKIP

Answer: C

NEW QUESTION 114

You work as a Network Administrator for NetTech Inc. When you enter <http://66.111.64.227> in the browser's address bar, you are able to access the site. But, you are unable to access the site when you enter <http://www.company.com>. What is the most likely cause?

- A. The site's Web server is offlin
- B. The site's Web server has heavy traffi
- C. WINS server has no NetBIOS name entry for the serve
- D. DNS entry is not available for the host nam

Answer: D

NEW QUESTION 119

What are the benefits of using AAA security service in a network? Each correct answer represents a part of the solution. Choose all that apply.

- A. It provides scalabilit
- B. It supports a single backup syste
- C. It increases flexibility and control of access configuratio
- D. It supports RADIUS, TACACS+, and Kerberos authentication method

Answer: ACD

NEW QUESTION 124

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

- A. Service-oriented logical design modeling
- B. Service-oriented conceptual architecture modeling
- C. Service-oriented discovery and analysis modeling
- D. Service-oriented business integration modeling

Answer: A

NEW QUESTION 127

Which of the following authentication methods support mutual authentication? Each correct answer represents a complete solution. Choose two.

- A. MS-CHAP v2
- B. NTLM
- C. EAP-MD5
- D. EAP-TLS

Answer: AD

NEW QUESTION 132

Which of the following keys is derived from a preshared key and Extensible Authentication Protocol (EAP)?

- A. Pairwise Transient Key
- B. Group Temporal Key
- C. Private Key
- D. Pairwise Master Key

Answer: D

NEW QUESTION 137

You work as a Network Administrator for Net World Inc. You are required to configure a VLAN for the company. Which of the following devices will you use to physically connect the computers in the VLAN? Each correct answer represents a complete solution. Choose two.

- A. Switch
- B. Router
- C. Bridge
- D. Hub
- E. Repeater

Answer: AB

NEW QUESTION 138

Which of the following protocols work at the Network layer of the OSI model?

- A. Routing Information Protocol (RIP)
- B. File Transfer Protocol (FTP)
- C. Simple Network Management Protocol (SNMP)
- D. Internet Group Management Protocol (IGMP)

Answer: AD

NEW QUESTION 142

Which of the following are used to suppress paper or wood fires? Each correct answer represents a complete solution. Choose two.

- A. Soda acid
- B. Kerosene
- C. Water
- D. CO2

Answer: AC

NEW QUESTION 146

Which of the following heights of fence deters only casual trespassers?

- A. 8 feet
- B. 3 to 4 feet
- C. 2 to 2.5 feet
- D. 6 to 7 feet

Answer: B

NEW QUESTION 149

In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

- A. Chosen plaintext attack
- B. Ciphertext only attack
- C. Chosen ciphertext attack
- D. Known plaintext attack

Answer: B

NEW QUESTION 151

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Annualized Rate of Occurrence (ARO)
- C. Single Loss Expectancy (SLE)
- D. Exposure Factor (EF)

Answer: B

NEW QUESTION 153

You work as a Chief Security Officer for Tech Perfect Inc. The company has a TCP/IP based network. You want to use a firewall that can track the state of active connections of the network and then determine which network packets are allowed to enter through the firewall. Which of the following firewalls has this feature?

- A. Stateful packet inspection firewall
- B. Proxy-based firewall
- C. Dynamic packet-filtering firewall
- D. Application gateway firewall

Answer: C

NEW QUESTION 157

Which of the following is a network service that stores and organizes information about a network users and network resources and that allows administrators to manage users' access to the resources?

- A. SMTP service
- B. Terminal service
- C. Directory service
- D. DFS service

Answer: C

NEW QUESTION 159

Which of the following are types of asymmetric encryption algorithms? Each correct answer represents a complete solution. Choose two.

- A. RSA
- B. AES
- C. ECC
- D. DES

Answer: AC

NEW QUESTION 162

Which of the following attacks allows the bypassing of access control lists on servers or routers, and helps an attacker to hide? Each correct answer represents a complete solution. Choose two.

- A. DNS cache poisoning
- B. MAC spoofing
- C. IP spoofing attack
- D. DDoS attack

Answer: BC

NEW QUESTION 167

You are the Network Administrator at a large company. Your company has a lot of contractors and other outside parties that come in and out of the building. For this reason you are concerned that simply having usernames and passwords is not enough and want to have employees use tokens for authentication. Which of the following is not an example of tokens?

- A. Smart card
- B. USB device with cryptographic data
- C. CHAP
- D. Key fob

Answer: C

NEW QUESTION 172

Which of the following components come under the network layer of the OSI model? Each correct answer represents a complete solution. Choose two.

- A. Routers
- B. MAC addresses
- C. Firewalls
- D. Hub

Answer: AC

NEW QUESTION 173

Which of the following are examples of physical controls used to prevent unauthorized access to sensitive materials?

- A. Thermal alarm systems
- B. Security Guards
- C. Closed circuit cameras
- D. Encryption

Answer: ABC

NEW QUESTION 176

Which of the following statements about Discretionary Access Control List (DACL) is true?

- A. It specifies whether an audit activity should be performed when an object attempts to access a resource
- B. It is a unique number that identifies a user, group, and computer account
- C. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object
- D. It is a rule list containing access control entries

Answer: C

NEW QUESTION 177

Which of the following methods will allow data to be sent on the Internet in a secure format?

- A. Serial Line Interface Protocol
- B. Point-to-Point Protocol
- C. Browsing
- D. Virtual Private Networks

Answer: D

NEW QUESTION 179

Which of the following are used to suppress electrical and computer fires? Each correct answer represents a complete solution. Choose two.

- A. Halon
- B. Water
- C. CO2
- D. Soda acid

Answer: AC

NEW QUESTION 181

Which of the following are natural environmental threats that an organization faces? Each correct answer represents a complete solution. Choose two.

- A. Strikes
- B. Floods
- C. Accidents
- D. Storms

Answer: BD

NEW QUESTION 182

Which of the following keys are included in a certificate revocation list (CRL) of a public key infrastructure (PKI)? Each correct answer represents a complete solution. Choose two.

- A. A foreign key
- B. A private key
- C. A public key
- D. A primary key

Answer: BC

NEW QUESTION 187

You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. You need to configure a firewall for the company. The firewall should be able to keep track of the state of network connections traveling across the network. Which of the following types of firewalls will you configure to accomplish the task?

- A. Stateful firewall
- B. Host-based application firewall
- C. A network-based application layer firewall
- D. An application firewall

Answer: A

NEW QUESTION 192

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

- A. Disaster recovery plan
- B. Contingency plan
- C. Business continuity plan
- D. Crisis communication plan

Answer: C

NEW QUESTION 197

Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

- A. Spoofing
- B. Packet sniffing
- C. Tunneling
- D. Packet filtering

Answer: C

NEW QUESTION 198

You work as a Security Manager for Tech Perfect Inc. A number of people are involved with you in the DRP efforts. You have maintained several different types of plan documents, intended for different audiences. Which of the following documents will be useful for you as well as public relations personnel who require a non-technical perspective on the entire organization's disaster recovery efforts?

- A. Technical guide
- B. Executive summary
- C. Checklist
- D. Department-specific plan

Answer: B

NEW QUESTION 203

Which of the following statements are true about Public-key cryptography? Each correct answer represents a complete solution. Choose two.

- A. Data encrypted with the secret key can only be decrypted by another secret key
- B. The secret key can encrypt a message, and anyone with the public key can decrypt it
- C. The distinguishing technique used in public key-private key cryptography is the use of symmetric key algorithm
- D. Data encrypted by the public key can only be decrypted by the secret key

Answer: BD

NEW QUESTION 208

In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

- A. Initiation
- B. Programming and training
- C. Design
- D. Evaluation and acceptance

Answer: B

NEW QUESTION 212

You are the administrator for YupNo.com. You want to increase and enhance the security of your computers and simplify deployment. You are especially concerned with any portable computers that are used by remote employees. What can you use to increase security, while still allowing your users to perform critical tasks?

- A. BitLocker
- B. Smart Cards
- C. Service Accounts
- D. AppLocker

Answer: B

NEW QUESTION 215

Which of the following uses public key cryptography to encrypt the contents of files?

- A. EFS
- B. DFS
- C. NTFS
- D. RFS

Answer: A

NEW QUESTION 220

You are responsible for security at a defense contracting firm. You are evaluating various possible encryption algorithms to use. One of the algorithms you are examining is not integer based, uses shorter keys, and is public key based. What type of algorithm is this?

- A. Symmetric
- B. None - all encryptions are integer base
- C. Elliptic Curve
- D. RSA

Answer: C

NEW QUESTION 222

Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

- A. $SLE = \text{Asset Value (AV)} * \text{Exposure Factor (EF)}$
- B. $SLE = \text{Asset Value (AV)} * \text{Annualized Rate of Occurrence (ARO)}$
- C. $SLE = \text{Annualized Loss Expectancy (ALE)} * \text{Annualized Rate of Occurrence (ARO)}$
- D. $SLE = \text{Annualized Loss Expectancy (ALE)} * \text{Exposure Factor (EF)}$

Answer: A

NEW QUESTION 224

Which of the following are man-made threats that an organization faces? Each correct answer represents a complete solution. Choose three.

- A. Theft
- B. Employee errors
- C. Strikes
- D. Frauds

Answer: ABD

NEW QUESTION 225

In which of the following access control models, owner of an object decides who is allowed to access the object and what privileges they have?

- A. Access Control List (ACL)
- B. Mandatory Access Control (MAC)
- C. Role Based Access Control (RBAC)
- D. Discretionary Access Control (DAC)

Answer: D

NEW QUESTION 229

Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

- A. Eradication phase
- B. Recovery phase
- C. Containment phase
- D. Preparation phase
- E. Identification phase

Answer: D

NEW QUESTION 230

Which of the following is an entry in an object's discretionary access control list (DACL) that grants permissions to a user or group?

- A. Access control entry (ACE)
- B. Discretionary access control entry (DACE)
- C. Access control list (ACL)
- D. Security Identifier (SID)

Answer: A

NEW QUESTION 231

Access control systems enable an authority to control access to areas and resources in a given physical facility or computer-based information system. Which of the following services provided by access control systems is used to determine what a subject can do?

- A. Authentication
- B. Authorization
- C. Accountability
- D. Identification

Answer: B

NEW QUESTION 232

You work as a Security Manager for Tech Perfect Inc. The management tells you to implement a hashing method in the organization that can resist forgery and is not open to the man-in-the-middle attack. Which of the following methods will you use to accomplish the task?

- A. MD
- B. NTLM
- C. MAC
- D. SHA

Answer: C

NEW QUESTION 236

Which of the following decides access control on an object in the mandatory access control (MAC) environment?

- A. Sensitivity label
- B. Event log
- C. System Access Control List (SACL)
- D. Security log

Answer: A

NEW QUESTION 240

Which of the following protocols supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection?

- A. PPTP
- B. UDP
- C. IPSec
- D. PAP

Answer: A

NEW QUESTION 242

You work as a remote support technician. A user named Rick calls you for support. Rick wants to connect his LAN connection to the Internet. Which of the following devices will you suggest that he use?

- A. Hub
- B. Repeater
- C. Bridge
- D. Switch
- E. Router

Answer: E

NEW QUESTION 244

Which of the following user authentications are supported by the SSH-1 protocol but not by the SSH-2 protocol? Each correct answer represents a complete solution. Choose all that apply.

- A. TIS authentication
- B. Rhosts (rsh-style) authentication
- C. Kerberos authentication
- D. Password-based authentication

Answer: ABC

NEW QUESTION 249

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

- A. Install a network-based IDS
- B. Install a host-based IDS
- C. Install a DMZ firewall
- D. Enable verbose logging on the firewall

Answer: A

NEW QUESTION 253

John works as an Ethical Hacker for company Inc. He wants to find out the ports that are open in company's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

- A. TCP FIN
- B. Xmas tree
- C. TCP SYN/ACK
- D. TCP SYN

Answer: D

NEW QUESTION 255

Which of the following is an infrastructure system that allows the secure exchange of data over an unsecured network?

- A. PMK
- B. PTK
- C. PKI
- D. GTK

Answer: C

NEW QUESTION 260

Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

- A. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer
- B. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer
- C. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer
- D. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

Answer: D

NEW QUESTION 265

Which of the following ports must be opened on the firewall for the VPN connection using Point-to-Point Tunneling Protocol (PPTP)?

- A. TCP port 110
- B. TCP port 443
- C. TCP port 5060
- D. TCP port 1723

Answer: D

NEW QUESTION 270

Which of the following techniques can be used by an administrator while working with the symmetric encryption cryptography? Each correct answer represents a complete solution. Choose all that apply.

- A. Block cipher
- B. Stream cipher
- C. Transposition cipher
- D. Message Authentication Code

Answer: ABD

NEW QUESTION 274

Which of the following authentication protocols sends a user certificate inside an encrypted tunnel?

- A. PEAP
- B. EAP-TLS
- C. WEP
- D. EAP-FAST

Answer: B

NEW QUESTION 276

You work as a Network Administrator for NetTech Inc. The company's network is connected to the Internet. For security, you want to restrict unauthorized access to the network with minimum administrative effort. You want to implement a hardware-based solution. What will you do to accomplish this?

- A. Connect a brouter to the network
- B. Implement a proxy server on the network
- C. Connect a router to the network
- D. Implement firewall on the network

Answer: D

NEW QUESTION 281

The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

- A. Service-oriented business integration modeling
- B. Service-oriented logical design modeling
- C. Service-oriented discovery and analysis modeling
- D. Service-oriented logical architecture modeling

Answer: D

NEW QUESTION 283

You are responsible for security at a building that has a lot of traffic. There are even a significant number of non-employees coming in and out of the building. You are concerned about being able to find out who is in the building at a particular time. What is the simplest way to accomplish this?

- A. Implement a sign in sheet at the main entrance and route all traffic through there
- B. Have all people entering the building use smart cards for access
- C. Implement biometric access
- D. Implement cameras at all entrance

Answer: A

NEW QUESTION 284

Which of the following methods of encryption uses a single key to encrypt and decrypt data?

- A. Asymmetric
- B. Symmetric
- C. S/MIME
- D. PGP

Answer: B

NEW QUESTION 287

Which of the following authentication methods provides credentials that are only valid during a single session?

- A. Kerberos v5
- B. Smart card
- C. Certificate
- D. Token

Answer: D

NEW QUESTION 289

Perfect World Inc., provides its sales managers access to the company's network from remote locations. The sales managers use laptops to connect to the network. For security purposes, the company's management wants the sales managers to log on to the network using smart cards over a remote connection. Which of the following authentication protocols should be used to accomplish this?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- C. Open Shortest Path First (OSPF)
- D. Extensible Authentication Protocol (EAP)

Answer: D

NEW QUESTION 293

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transfer
- D. Risk mitigation

Answer: C

NEW QUESTION 297

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CISSP-ISSAP Practice Exam Features:

- * CISSP-ISSAP Questions and Answers Updated Frequently
- * CISSP-ISSAP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP-ISSAP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP-ISSAP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP-ISSAP Practice Test Here](#)