

ISC2

Exam Questions ISSAP

ISSAP Information Systems Security Architecture Professional



NEW QUESTION 1

- (Exam Topic 1)

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol? Each correct answer represents a complete solution. Choose all that apply.

- A. Blowfish
- B. DES
- C. IDEA
- D. RC4

Answer: ABC

NEW QUESTION 2

- (Exam Topic 1)

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 3

- (Exam Topic 1)

Which of the following terms refers to the method that allows or restricts specific types of packets from crossing over the firewall?

- A. Hacking
- B. Packet filtering
- C. Web caching
- D. Spoofing

Answer: B

NEW QUESTION 4

- (Exam Topic 1)

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

- (Exam Topic 1)

Which of the following firewalls inspects the actual contents of packets?

- A. Packet filtering firewall
- B. Stateful inspection firewall
- C. Application-level firewall
- D. Circuit-level firewall

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

Which of the following types of firewall functions at the Session layer of OSI model?

- A. Circuit-level firewall
- B. Application-level firewall
- C. Packet filtering firewall
- D. Switch-level firewall

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

The IPSec protocol is configured in an organization's network in order to maintain a complete infrastructure for secured network communications. IPSec uses four components for this. Which of the following components reduces the size of data transmitted over congested network connections and increases the speed of such networks without losing data?

- A. AH

- B. ESP
- C. IPcomp
- D. IKE

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

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 9

- (Exam Topic 1)

Which of the following is used to authenticate asymmetric keys?

- A. Digital signature
- B. MAC Address
- C. Demilitarized zone (DMZ)
- D. Password

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

Which of the following types of attack can be used to break the best physical and logical security mechanism to gain access to a system?

- A. Social engineering attack
- B. Cross site scripting attack
- C. Mail bombing
- D. Password guessing attack

Answer: A

NEW QUESTION 15

- (Exam Topic 1)

Which of the following statements about Public Key Infrastructure (PKI) are true? Each correct answer represents a complete solution. Choose two.

- A. It uses symmetric key pairs.
- B. It provides security using data encryption and digital signature.
- C. It uses asymmetric key pairs.
- D. It is a digital representation of information that identifies users.

Answer: BC

NEW QUESTION 19

- (Exam Topic 1)

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 24

- (Exam Topic 1)

IPsec VPN provides a high degree of data privacy by establishing trust points between communicating devices and data encryption. Which of the following encryption methods does IPsec VPN use? Each correct answer represents a complete solution. Choose two.

- A. MD5
- B. LEAP
- C. AES
- D. 3DES

Answer: CD

NEW QUESTION 28

- (Exam Topic 1)

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 32

- (Exam Topic 1)

Computer networks and the Internet are the prime mode of Information transfer today. 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. Firewall security
- C. Cryptography
- D. OODA loop

Answer: C

NEW QUESTION 33

- (Exam Topic 1)

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 35

- (Exam Topic 1)

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 38

- (Exam Topic 1)

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 42

- (Exam Topic 1)

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 45

- (Exam Topic 1)

Sam is creating an e-commerce site. He wants a simple security solution that does not require each customer to have an individual key. Which of the following encryption methods will he use?

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

Answer: B

NEW QUESTION 48

- (Exam Topic 1)

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 51

- (Exam Topic 1)

Peter works as a Network Administrator for Net World Inc. The company wants to allow remote users to connect and access its private network through a dial-up connection via the Internet. All the data will be sent across a public network. For security reasons, the management wants the data sent through the Internet to be encrypted. The company plans to use a Layer 2 Tunneling Protocol (L2TP) connection. Which communication protocol will Peter use to accomplish the task?

- A. IP Security (IPSec)
- B. Microsoft Point-to-Point Encryption (MPPE)
- C. Pretty Good Privacy (PGP)
- D. Data Encryption Standard (DES)

Answer: A

NEW QUESTION 55

- (Exam Topic 1)

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 59

- (Exam Topic 1)

Mark has been hired by a company to work as a Network Assistant. He is assigned the task to configure a dial-up connection. He is configuring a laptop. Which of the following protocols should he disable to ensure that the password is encrypted during remote access?

- A. SPAP
- B. MSCHAP
- C. PAP
- D. MSCHAP V2

Answer: C

NEW QUESTION 60

- (Exam Topic 1)

You are the Network Administrator for a college. You watch a large number of people (some not even students) going in and out of areas with campus computers (libraries, computer labs, etc.). You have had a problem with laptops being stolen. What is the most cost effective method to prevent this?

- A. Smart card access to all areas with computers.
- B. Use laptop locks.
- C. Video surveillance on all areas with computers.
- D. Appoint a security guard.

Answer: B

NEW QUESTION 65

- (Exam Topic 2)

You work as an administrator for Techraft Inc. Employees of your company create 'products', which are supposed to be given different levels of access. You need to configure a security policy in such a way that an employee (producer of the product) grants accessing privileges (such as read, write, or alter) for his product. Which of the following access control models will you use to accomplish this task?

- A. Discretionary access control (DAC)
- B. Role-based access control (RBAC)
- C. Mandatory access control (MAC)
- D. Access control list (ACL)

Answer: A

NEW QUESTION 67

- (Exam Topic 2)

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 68

- (Exam Topic 2)

Your customer is concerned about security. He wants to make certain no one in the outside world can see the IP addresses inside his network. What feature of a router would accomplish this?

- A. Port forwarding
- B. NAT
- C. MAC filtering
- D. Firewall

Answer: B

NEW QUESTION 69

- (Exam Topic 2)

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 70

- (Exam Topic 2)

Which of the following types of ciphers operates on a group of bits rather than an individual character or bit of a message?

- A. Block cipher
- B. Classical cipher
- C. Substitution cipher
- D. Stream cipher

Answer: A

NEW QUESTION 73

- (Exam Topic 2)

You work as a Chief Security Officer for Tech Perfect Inc. You have configured IPSec and ISAKMP protocol in the company's network in order to establish a secure communication infrastructure. According to the Internet RFC 2408, which of the following services does the ISAKMP protocol offer to the network? Each correct answer represents a part of the solution. Choose all that apply.

- A. It relies upon a system of security associations.
- B. It provides key generation mechanisms.
- C. It authenticates communicating peers.
- D. It protects against threats, such as DoS attack, replay attack, etc.

Answer: BCD

NEW QUESTION 74

- (Exam Topic 2)

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 75

- (Exam Topic 2)

Which of the following processes identifies the threats that can impact the business continuity of operations?

- A. Function analysis
- B. Risk analysis
- C. Business impact analysis
- D. Requirement analysis

Answer: C

NEW QUESTION 80

- (Exam Topic 2)

Which of the following are the centralized administration technologies? Each correct answer represents a complete solution. Choose all that apply.

- A. RADIUS
- B. TACACS+
- C. Media Access control
- D. Peer-to-Peer

Answer: AB

NEW QUESTION 82

- (Exam Topic 2)

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 85

- (Exam Topic 2)

The OSI reference model is divided into layers and each layer has a specific task to perform. At which layer of OSI model is the File and Print service performed?

- A. Session layer
- B. Presentation layer
- C. Transport layer
- D. Application layer

Answer: D

NEW QUESTION 87

- (Exam Topic 2)

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 92

- (Exam Topic 2)

You work as a Chief Security Officer for Tech Perfect Inc. The company has an internal room without any window and is totally in darkness. For security reasons, you want to place a device in the room. Which of the following devices is best for that room?

- A. Photoelectric motion detector
- B. Badge
- C. Closed-circuit television
- D. Alarm

Answer: A

NEW QUESTION 94

- (Exam Topic 2)

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

- A. Twofish
- B. Digital certificates
- C. Public key
- D. RSA

Answer: BC

NEW QUESTION 95

- (Exam Topic 2)

Which of the following backup types backs up files that have been added and all data that have been modified since the most recent backup was performed?

- A. Differential backup
- B. Incremental backup
- C. Daily backup
- D. Full backup

Answer: B

NEW QUESTION 99

- (Exam Topic 2)

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 101

- (Exam Topic 2)

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 offline.
- B. The site's Web server has heavy traffic.
- C. WINS server has no NetBIOS name entry for the server.
- D. DNS entry is not available for the host name.

Answer: D

NEW QUESTION 104

- (Exam Topic 2)

Which of the following are the phases of the Certification and Accreditation (C&A) process? Each correct answer represents a complete solution. Choose two.

- A. Detection
- B. Continuous Monitoring
- C. Initiation
- D. Auditing

Answer: BC

NEW QUESTION 109

- (Exam Topic 2)

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You have a disaster scenario and you want to discuss it with your team members for getting appropriate responses of the disaster. In which of the following disaster recovery tests can this task be performed?

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

Answer: C

NEW QUESTION 114

- (Exam Topic 2)

You are implementing some security services in an organization, such as smart cards, biometrics, access control lists, firewalls, intrusion detection systems, and clipping levels. Which of the following categories of implementation of the access control includes all these security services?

- A. Administrative access control
- B. Logical access control
- C. Physical access control
- D. Preventive access control

Answer: B

NEW QUESTION 117

- (Exam Topic 2)

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 122

- (Exam Topic 2)

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

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

Answer: D

NEW QUESTION 124

- (Exam Topic 2)

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 125

- (Exam Topic 2)

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 127

- (Exam Topic 2)

You are calculating the Annualized Loss Expectancy (ALE) using the following formula: $ALE = AV * EF * ARO$ What information does the AV (Asset Value) convey?

- A. It represents how many times per year a specific threat occurs.
- B. It represents the percentage of loss that an asset experiences if an anticipated threat occurs.
- C. It is expected loss for an asset due to a risk over a one year period.
- D. It represents the total cost of an asset, including the purchase price, recurring maintenance, expenses, and all other costs.

Answer: D

NEW QUESTION 128

- (Exam Topic 2)

In which of the following SDLC phases are the software and other components of the system faithfully incorporated into the design specifications?

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

Answer: A

NEW QUESTION 130

- (Exam Topic 2)

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 134

- (Exam Topic 2)

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 137

- (Exam Topic 2)

Which of the following password authentication schemes enables a user with a domain account to log on to a network once, using a password or smart card, and to gain access to multiple computers in the domain without being prompted to log in again?

- A. Single Sign-On
- B. One-time password
- C. Dynamic
- D. Kerberos

Answer: A

NEW QUESTION 142

- (Exam Topic 2)

You work as a Network Consultant. A company named Tech Perfect Inc. hires you for security reasons. The manager of the company tells you to establish connectivity between clients and servers of the network which prevents eavesdropping and tampering of data on the Internet. Which of the following will you configure on the network to perform the given task?

- A. WEP
- B. IPsec
- C. VPN
- D. SSL

Answer: D

NEW QUESTION 144

- (Exam Topic 2)

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 148

- (Exam Topic 2)

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 153

- (Exam Topic 2)

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 formatting
- B. These layers reside at the top of the model.
- C. Layers 4 through 7 define the functionality of IP Addressing, Physical Standards, and Data Link protocols.

- D. Layers 5, 6, and 7 focus on the Network Application, which includes data formatting and session control.
E. Layers 1, 2, 3, and 4 deal with physical connectivity, encapsulation, IP Addressing, and Error Recovery. These layers define the end-to-end functions of data delivery.

Answer: CD

NEW QUESTION 157

- (Exam Topic 2)

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

- A. Parallel test
- B. Simulation test
- C. Full-interruption test
- D. Checklist test

Answer: D

NEW QUESTION 160

- (Exam Topic 2)

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 algorithms.
- D. Data encrypted by the public key can only be decrypted by the secret key.

Answer: BD

NEW QUESTION 163

- (Exam Topic 2)

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 164

- (Exam Topic 2)

Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation

- A. Design
- B. Maintenance
- C. Deployment
- D. Requirements Gathering

Answer: A

NEW QUESTION 165

- (Exam Topic 2)

You work as a Network Administrator for McNeil Inc. The company has a TCP/IP-based network. Performance of the network is slow because of heavy traffic. A hub is used as a central connecting device in the network. Which of the following devices can be used in place of a hub to control the network traffic efficiently?

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

Answer: C

NEW QUESTION 168

- (Exam Topic 2)

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 173

- (Exam Topic 2)

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 174

- (Exam Topic 2)

Adam works as a Network Administrator. He discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. Which of the following types of authentication mechanism is used here?

- A. Pre-shared key authentication
- B. Open system authentication
- C. Shared key authentication
- D. Single key authentication

Answer: C

NEW QUESTION 178

- (Exam Topic 2)

The security controls that are implemented to manage physical security are divided in various groups. Which of the following services are offered by the administrative physical security control group? Each correct answer represents a part of the solution. Choose all that apply.

- A. Construction and selection
- B. Site management
- C. Awareness training
- D. Access control
- E. Intrusion detection
- F. Personnel control

Answer: ABCF

NEW QUESTION 182

.....

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

ISSAP Practice Exam Features:

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

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