

# ISC2

## Exam Questions ISSAP

ISSAP Information Systems Security Architecture Professional



#### NEW QUESTION 1

- (Exam Topic 1)

Which of the following statements about a stream cipher are true? Each correct answer represents a complete solution. Choose three.

- A. It typically executes at a higher speed than a block cipher.
- B. It divides a message into blocks for processing.
- C. It typically executes at a slower speed than a block cipher.
- D. It divides a message into bits for processing.
- E. It is a symmetric key cipher.

**Answer:** ADE

#### NEW QUESTION 2

- (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 3

- (Exam Topic 1)

Which of the following are the primary components of a discretionary access control (DAC) model? Each correct answer represents a complete solution. Choose two.

- A. User's group
- B. File and data ownership
- C. Smart card
- D. Access rights and permissions

**Answer:** BD

#### 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)

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

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

**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)

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 8

- (Exam Topic 1)

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 9

- (Exam Topic 1)

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 used.
- 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 used.

**Answer:** CD

#### NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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 14

- (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 19

- (Exam Topic 1)

You want to connect a twisted pair cable segment to a fiber-optic cable segment. Which of the following networking devices will you use to accomplish the task?

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

**Answer:** C

**NEW QUESTION 23**

- (Exam Topic 1)

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 26**

- (Exam Topic 1)

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 30**

- (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 33**

- (Exam Topic 1)

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 38**

- (Exam Topic 1)

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**

- (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 45**

- (Exam Topic 1)

Which of the following protocols provides connectionless integrity and data origin authentication of IP packets?

- A. ESP
- B. AH
- C. IKE
- D. ISAKMP

**Answer:** B

#### NEW QUESTION 50

- (Exam Topic 1)

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem. Which of the following utilities will you use to diagnose the problem?

- A. TRACERT
- B. PING
- C. IPCONFIG
- D. NSLOOKUP

**Answer:** D

#### NEW QUESTION 54

- (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 58

- (Exam Topic 1)

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 61

- (Exam Topic 1)

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 laptops.
- B. Keeping all doors locked with a guard.
- C. Using a man-trap.
- D. A sign in log.

**Answer:** C

#### NEW QUESTION 64

- (Exam Topic 1)

Which of the following is a method for transforming a message into a masked form, together with a way of undoing the transformation to recover the message?

- A. Cipher
- B. CrypTool
- C. Steganography
- D. MIME

**Answer:** A

#### NEW QUESTION 68

- (Exam Topic 1)

A helpdesk technician received a phone call from an administrator at a remote branch office. The administrator claimed to have forgotten the password for the root account on UNIX servers and asked for it. Although the technician didn't know any administrator at the branch office, the guy sounded really friendly and since he knew the root password himself, he supplied the caller with the password. What type of attack has just occurred?

- A. Social Engineering attack
- B. Brute Force attack
- C. War dialing attack
- D. Replay attack

**Answer:** A

#### NEW QUESTION 72

- (Exam Topic 1)

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 77

- (Exam Topic 1)

Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

- A. RCO
- B. RTO
- C. RPO
- D. RTA

**Answer:** B

#### NEW QUESTION 81

- (Exam Topic 1)

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 83

- (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 87

- (Exam Topic 1)

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 92

- (Exam Topic 1)

Which of the following protocols uses the Internet key Exchange (IKE) protocol to set up security associations (SA)?

- A. IPSec
- B. L2TP
- C. LEAP
- D. ISAKMP

**Answer:** D

#### NEW QUESTION 96

- (Exam Topic 1)

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 98

- (Exam Topic 1)

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

- A. Authentication
- B. Non-repudiation
- C. Integrity
- D. Confidentiality

**Answer:** D

#### NEW QUESTION 100

- (Exam Topic 1)

Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme? Each correct answer represents a complete solution. Choose all that apply.

- A. Kerberos requires continuous availability of a central server.
- B. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's passwords.
- C. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.
- D. Kerberos requires the clocks of the involved hosts to be synchronized.

**Answer:** ABD

#### NEW QUESTION 103

- (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 107

- (Exam Topic 1)

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 112

- (Exam Topic 1)

In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

- A. Hot Site
- B. Mobile Site
- C. Warm Site
- D. Cold Site

**Answer:** A

#### NEW QUESTION 115

- (Exam Topic 1)

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 117

- (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 119

- (Exam Topic 2)

Which of the following cables provides maximum security against electronic eavesdropping on a network?

- A. Fibre optic cable
- B. STP cable
- C. UTP cable
- D. NTP cable

**Answer:** A

#### NEW QUESTION 122

- (Exam Topic 2)

Which of the following methods for identifying appropriate BIA interviewees' includes examining the organizational chart of the enterprise to understand the functional positions?

- A. Executive management interviews
- B. Overlaying system technology
- C. Organizational chart reviews
- D. Organizational process models

**Answer:** C

#### NEW QUESTION 124

- (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 127

- (Exam Topic 2)

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 128

- (Exam Topic 2)

You work as a Network Administrator for company Inc. The company has deployed an ASA at the network perimeter. Which of the following types of firewall will you use to create two different communications, one between the client and the firewall, and the other between the firewall and the end server?

- A. Stateful firewall
- B. Endian firewall
- C. Packet filter firewall
- D. Proxy-based firewall



**Answer:** D

**NEW QUESTION 130**

- (Exam Topic 2)

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 133**

- (Exam Topic 2)

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 134**

- (Exam Topic 2)

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 138**

- (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 140**

- (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 145**

- (Exam Topic 2)

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 147**

- (Exam Topic 2)

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 151**

- (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 153**

- (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 157**

- (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 159**

- (Exam Topic 2)

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 based.
- C. Elliptic Curve
- D. RSA

**Answer:** C

**NEW QUESTION 160**

- (Exam Topic 2)

Which of the following protocols provides the highest level of VPN security with a VPN connection that uses the L2TP protocol?

- A. IPSec
- B. PPPoE
- C. PPP
- D. TFTP

**Answer:** A

**NEW QUESTION 164**

- (Exam Topic 2)

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 scalability.
- B. It supports a single backup system.
- C. It increases flexibility and control of access configuration.
- D. It supports RADIUS, TACACS+, and Kerberos authentication methods.

**Answer:** ACD

**NEW QUESTION 167**

- (Exam Topic 2)

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

- A. Warm site
- B. Cold site
- C. Off site
- D. Hot site

**Answer:** B

#### NEW QUESTION 169

- (Exam Topic 2)

You are the Security Administrator for a consulting firm. One of your clients needs to encrypt traffic. However, he has specific requirements for the encryption algorithm. It must be a symmetric key block cipher.

Which of the following should you choose for this client?

- A. PGP
- B. SSH
- C. DES
- D. RC4

**Answer:** C

#### NEW QUESTION 173

- (Exam Topic 2)

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Which of the following components does the PKI use to list those certificates that have been revoked or are no longer valid?

- A. Certification Practice Statement
- B. Certificate Policy
- C. Certificate Revocation List
- D. Certification Authority

**Answer:** C

#### NEW QUESTION 175

- (Exam Topic 2)

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 176

- (Exam Topic 2)

Fill in the blank with the appropriate encryption system. The \_\_\_\_\_ encryption system is an asymmetric key encryption algorithm for the public-key cryptography, which is based on the Diffie- Hellman key agreement.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

ElGamal

#### NEW QUESTION 180

- (Exam Topic 2)

A company named Money Builders Inc., hires you to provide consultancy for setting up their Windows network. The company's server room will be in a highly secured environment. You are required to suggest an authentication method for it. The CFO of the company wants the server to use thumb impressions for authentication. Which of the following authentication methods will you suggest?

- A. Certificate
- B. Smart card
- C. Two-factor
- D. Biometrics

**Answer:** D

#### NEW QUESTION 183

- (Exam Topic 2)

In software development, which of the following analysis is used to document the services and functions that have been accidentally left out, deliberately eliminated or still need to be developed?

- A. Gap analysis
- B. Requirement analysis
- C. Cost-benefit analysis
- D. Vulnerability analysis

**Answer:** A

#### NEW QUESTION 184

- (Exam Topic 2)

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 188

- (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 189

- (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 191

- (Exam Topic 2)

Mark works as a Network Administrator for NetTech Inc. He wants to connect the company's headquarter and its regional offices using a WAN technology. For this, he uses packet-switched connection. Which of the following WAN technologies will Mark use to connect the offices? Each correct answer represents a complete solution. Choose two.

- A. ISDN
- B. X.25
- C. Frame Relay
- D. Leased line

**Answer:** BC

#### NEW QUESTION 193

- (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 195

- (Exam Topic 2)

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**

- (Exam Topic 2)

Which of the following algorithms can be used to check the integrity of a file? 158

Each correct answer represents a complete solution. Choose two.

- A. md5
- B. rsa
- C. blowfish
- D. sha

**Answer:** AD

**NEW QUESTION 200**

- (Exam Topic 2)

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 205**

- (Exam Topic 2)

Which of the following authentication methods is based on physical appearance of a user?

- A. Key fob
- B. Biometrics
- C. ID/password combination
- D. Smart card

**Answer:** B

**NEW QUESTION 206**

- (Exam Topic 2)

Which of the following layers of the OSI model provides non-repudiation services?

- A. The application layer
- B. The data-link layer
- C. The presentation layer
- D. The physical layer

**Answer:** A

**NEW QUESTION 211**

- (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 212**

- (Exam Topic 2)

Which of the following are the goals of a public key infrastructure (PKI)? Each correct answer represents a part of the solution. Choose all that apply.

- A. Authenticity
- B. Globalization
- C. Mobility
- D. Integrity
- E. Confidentiality
- F. Nonrepudiation

**Answer:** ADEF

**NEW QUESTION 216**

- (Exam Topic 2)

Which of the following LAN protocols use token passing for exchanging signals among various stations on the network? Each correct answer represents a complete solution. Choose two.

- A. Ethernet (IEEE 802.3)
- B. Token ring (IEEE 802.5)
- C. Fiber Distributed Data Interface (FDDI)
- D. Wireless LAN (IEEE 802.11b)

**Answer:** BC

#### **NEW QUESTION 217**

- (Exam Topic 2)

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 222**

- (Exam Topic 2)

Which of the following is the most secure method of authentication?

- A. Smart card
- B. Anonymous
- C. Username and password
- D. Biometrics

**Answer:** D

#### **NEW QUESTION 226**

- (Exam Topic 2)

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 228**

- (Exam Topic 2)

Which of the following encryption methods comes under symmetric encryption algorithm? Each correct answer represents a complete solution. Choose three.

- A. DES
- B. Blowfish
- C. RC5
- D. Diffie-Hellman

**Answer:** ABC

#### **NEW QUESTION 229**

- (Exam Topic 2)

Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

- A. Kerberos
- B. Cryptography
- C. Cryptographer
- D. Cryptanalysis

**Answer:** D

#### **NEW QUESTION 233**

- (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 236

- (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 239

- (Exam Topic 2)

Which of the following describes the acceptable amount of data loss measured in time?

- A. Recovery Consistency Objective (RCO)
- B. Recovery Time Objective (RTO)
- C. Recovery Point Objective (RPO)
- D. Recovery Time Actual (RTA)

**Answer:** C

#### NEW QUESTION 241

- (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 244

- (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 249

- (Exam Topic 2)

Which of the following encryption algorithms is used by the Clipper chip, which supports the escrowed encryption standard?

- A. Skipjack
- B. Blowfish
- C. AES
- D. IDEA

**Answer:** A

#### NEW QUESTION 254

- (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 255

- (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 257

- (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 262

- (Exam Topic 2)

Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?

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

**Answer:** D

#### NEW QUESTION 267

- (Exam Topic 2)

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 271

- (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 275

- (Exam Topic 2)

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 280

- (Exam Topic 2)

Which of the following encryption modes has the property to allow many error correcting codes to function normally even when applied before encryption?

- A. OFB mode
- B. CFB mode
- C. CBC mode
- D. PCBC mode

**Answer:** A

#### NEW QUESTION 285

- (Exam Topic 2)

Which of the following uses a Key Distribution Center (KDC) to authenticate a principle?

- A. CHAP
- B. PAP
- C. Kerberos
- D. TACACS

**Answer:** C

#### NEW QUESTION 289

- (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 291

- (Exam Topic 2)

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 294

- (Exam Topic 2)

You are responsible for security at a hospital. Since many computers are accessed by multiple employees 24 hours a day, 7 days a week, controlling physical access to computers is very difficult. This is compounded by a high number of non employees moving through the building. You are concerned about unauthorized access to patient records. What would best solve this problem?

- A. The use of CHAP.
- B. Time of day restrictions.
- C. The use of smart cards.
- D. Video surveillance of all computers.

**Answer:** C

#### NEW QUESTION 297

- (Exam Topic 2)

Della works as a security manager for SoftTech Inc. She is training some of the newly recruited personnel in the field of security management. She is giving a tutorial on DRP. She explains that the major goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited personnel in SoftTech Inc, what will be your answer for her question? Each correct answer represents a part of the solution. Choose three.

- A. Guarantee the reliability of standby systems through testing and simulation.
- B. Protect an organization from major computer services failure.
- C. Minimize the risk to the organization from delays in providing services.
- D. Maximize the decision-making required by personnel during a disaster.

**Answer:** ABC

#### NEW QUESTION 302

- (Exam Topic 2)

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 305

- (Exam Topic 2)

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 306**

- (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 309**

- (Exam Topic 2)

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 310**

- (Exam Topic 2)

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 311**

- (Exam Topic 2)

An access control secures the confidentiality, integrity, and availability of the information and data of an organization. In which of the following categories can you deploy the access control? Each correct answer represents a part of the solution. Choose all that apply.

- A. Detective access control
- B. Corrective access control
- C. Administrative access control
- D. Preventive access control

**Answer:** ABD

**NEW QUESTION 315**

- (Exam Topic 2)

You work as a Network Administrator for McRoberts Inc. You are expanding your company's network. After you have implemented the network, you test the connectivity to a remote host by using the PING command. You get the ICMP echo reply message from the remote host. Which of the following layers of the OSI model are tested through this process? Each correct answer represents a complete solution. Choose all that apply.

- A. Layer 3
- B. Layer 2
- C. Layer 4
- D. Layer 1

**Answer:** ABD

**NEW QUESTION 318**

- (Exam Topic 2)

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 322

- (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 323

- (Exam Topic 2)

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 326

- (Exam Topic 2)

You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution? Each correct answer represents a part of the solution. Choose all that apply.

- A. Identification
- B. Eradication
- C. Recovery
- D. Contamination
- E. Preparation

**Answer:** BCD

#### NEW QUESTION 331

- (Exam Topic 2)

Sonya, a user, reports that she works in an electrically unstable environment where brownouts are a regular occurrence. Which of the following will you tell her to use to protect her computer?

- A. UPS
- B. Multimeter
- C. SMPS
- D. CMOS battery

**Answer:** A

#### NEW QUESTION 332

- (Exam Topic 2)

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 334

.....

## 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](#)**