ISC2

Exam Questions ISSAP

ISSAP Information Systems Security Architecture Professional

NEW QUESTION 1
- (Exam Topic 1)
Which of the following protocols multicasts messages and information among all member devices in an IP multicast group?

A. ARP
B. ICMP
C. TCP
D. IGMP

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
You have decided to implement video surveillance in your company in order to enhance network security. Which of the following locations must have a camera in order to provide the minimum level of security for the network resources? Each correct answer represents a complete solution. Choose two.

A. Parking lot
B. All hallways
C. Server Rooms
D. All offices
E. All entrance doors

Answer: CE

NEW QUESTION 3
- (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 4
- (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 5
- (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 6
- (Exam Topic 1)
Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

A. Estimate the potential losses to assets by determining their value.
B. Establish the threats likelihood and regularity.
C. Valuations of the critical assets in hard costs.
D. Evaluate potential threats to the assets.

Answer: ABD

NEW QUESTION 7
- (Exam Topic 1)
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. PPTP
C. IPSec
D. NTFS

Answer: A

NEW QUESTION 8
- (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 9
- (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)
An organization wants to allow a certificate authority to gain access to the encrypted data and create digital signatures on behalf of the user. The data is encrypted using the public key from a user's certificate. Which of the following processes fulfills the above requirements?

A. Key escrow
B. Key storage
C. Key revocation
D. Key recovery

Answer: A

NEW QUESTION 10
- (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 13
- (Exam Topic 1)
Which of the following statements best describes a certification authority?

A. A certification authority is a technique to authenticate digital documents by using computer cryptography.
B. A certification authority is a type of encryption that uses a public key and a private key pair for data encryption.
C. A certification authority is an entity that issues digital certificates for use by other parties.
D. A certification authority is a type of encryption that uses a single key to encrypt and decrypt data.

Answer: C

NEW QUESTION 14
- (Exam Topic 1)
Andrew works as a Network Administrator for Infonet Inc. The company's network has a Web server that hosts the company's Web site. Andrew wants to increase the security of the Web site by implementing Secure Sockets Layer (SSL). Which of the following types of encryption does SSL use? Each correct answer represents a complete solution. Choose two.

A. Synchronous
B. Secret
C. Asymmetric
D. Symmetric

Answer: CD

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 20
- (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 25
- (Exam Topic 1)
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 26
- (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 28
- (Exam Topic 1)
Which of the following encryption methods does the SSL protocol use in order to provide communication privacy, authentication, and message integrity? Each correct answer represents a part of the solution. Choose two.

A. Public key
B. IPsec
C. MS-CHAP
D. Symmetric

Answer: AD

NEW QUESTION 29
- (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 33
- (Exam Topic 1)
You have been assigned the task of selecting a hash algorithm. The algorithm will be specifically used to ensure the integrity of certain sensitive files. It must use a

128 bit hash value. Which of the following should you use?

A. AES
B. SHA
C. MD5
D. DES

Answer: C

NEW QUESTION 36
- (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 39
- (Exam Topic 1)
Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. Network-based
B. Anomaly-based
C. File-based
D. Signature-based

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
Which of the following encryption modes can make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way?

A. Cipher feedback mode
B. Cipher block chaining mode
C. Output feedback mode
D. Electronic codebook mode

Answer: D

NEW QUESTION 46
- (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 47
- (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 acchitecture
C. System access
D. Data backups

Answer: ABC

NEW QUESTION 49
- (Exam Topic 1)
Which of the following protocols is designed to efficiently handle high-speed data over wide area networks (WANs)?

A. PPP
B. X.25
C. Frame relay
D. SLIP

Answer: C

NEW QUESTION 53
- (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 55
- (Exam Topic 1)
Which of the following statements about incremental backup are true? Each correct answer represents a complete solution. Choose two.

A. It is the fastest method of backing up data.
B. It is the slowest method for taking a data backup.
C. It backs up the entire database, including the transaction log.
D. It backs up only the files changed since the most recent backup and clears the archive bit.

Answer: AD

NEW QUESTION 57
- (Exam Topic 1)
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

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

Answer: D

NEW QUESTION 62
- (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 66
- (Exam Topic 1)
Which of the following does PEAP use to authenticate the user inside an encrypted tunnel? Each correct answer represents a complete solution. Choose two.

A. GTC
B. MS-CHAP v2
C. AES
D. RC4

Answer: AB

NEW QUESTION 68
- (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 72
- (Exam Topic 2)
Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and

modeling?

A. Service-oriented modeling framework (SOMF)
B. Service-oriented modeling and architecture (SOMA)
C. Sherwood Applied Business Security Architecture (SABSA)
D. Service-oriented architecture (SOA)

Answer: A

NEW QUESTION 77
- (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 81
- (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 85
- (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 89
- (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 92
- (Exam Topic 2)
Which of the following is a form of gate that allows one person to pass at a time?

A. Biometric
B. Man-trap
C. Turnstile
D. Fence

Answer: C

NEW QUESTION 95
- (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 96
- (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 101
- (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 102
- (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 105
- (Exam Topic 2)
Which of the following encryption algorithms are based on block ciphers?

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

Answer: BCD

NEW QUESTION 110
- (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 111
- (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 112
- (Exam Topic 2)
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 114
- (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 115
- (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 116
- (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 120
- (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 122
- (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 125
- (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 129

- (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 132
- (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 134
- (Exam Topic 2)
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 135
- (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 140
- (Exam Topic 2)
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 141
- (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 142
- (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 145
- (Exam Topic 2)
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 148
- (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 150
- (Exam Topic 2)
John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

A. Evacuation drill
B. Walk-through drill
C. Structured walk-through test
D. Full-scale exercise

Answer: C

NEW QUESTION 151
- (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 153
- (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 154
- (Exam Topic 2)
In which of the following Person-to-Person social engineering attacks does an attacker pretend to be an outside contractor, delivery person, etc., in order to gain physical access to the organization?

A. In person attack
B. Third-party authorization attack

C. Impersonation attack
D. Important user posing attack

Answer: C

NEW QUESTION 155
- (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 157
- (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 159
- (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 163
- (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 166
- (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 170
- (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 175

- (Exam Topic 2)
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 178
- (Exam Topic 2)
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 182
- (Exam Topic 2)
You are the Security Consultant and have been contacted by a client regarding their encryption and hashing algorithms. Their in-house network administrator tells you that their current hashing algorithm is an older one with known weaknesses and is not collision resistant.Which algorithm are they most likely using for hashing?

A. PKI
B. SHA
C. Kerberos
D. MD5

Answer: D

NEW QUESTION 186
- (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 188
- (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 192
- (Exam Topic 2)
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 193
- (Exam Topic 2)
You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

A. Take a full backup daily and use six-tape rotation.

B. Take a full backup on Monday and a differential backup on each of the following weekday
C. Keep Monday's backup offsite.
D. Take a full backup daily with the previous night's tape taken offsite.
E. Take a full backup on alternate days and keep rotating the tapes.
F. Take a full backup on Monday and an incremental backup on each of the following weekday
G. Keep Monday's backup offsite.
H. Take a full backup daily with one tape taken offsite weekly.

Answer: C

NEW QUESTION 196
- (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 199
- (Exam Topic 2)
An organization has implemented a hierarchical-based concept of privilege management in which administrators have full access, HR managers have less permission than the administrators, and data entry operators have no access to resources. Which of the following access control models is implemented in the organization?

A. Role-based access control (RBAC)
B. Network-based access control (NBAC)
C. Mandatory Access Control (MAC)
D. Discretionary access control (DAC)

Answer: A

NEW QUESTION 202
- (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 204
- (Exam Topic 2)
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 entrances.

Answer: A

NEW QUESTION 205
- (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 207
- (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 211
- (Exam Topic 2)
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 214
- (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 215
- (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 220
- (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 223
- (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 227
- (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 228
- (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 231
- (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 236
- (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 240
- (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 245
- (Exam Topic 2)
In which of the following cryptographic attacking techniques does the attacker pick up the information to be encrypted and take a copy of it with the encrypted data?

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

Answer: C

NEW QUESTION 249
- (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 254
- (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 256
- (Exam Topic 2)
Which of the following schemes is used by the Kerberos authentication?

A. Public key cryptography
B. One time password
C. Private key cryptography
D. OPIE

Answer: C

NEW QUESTION 257
- (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 261
- (Exam Topic 2)
Which of the following are types of access control attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Dictionary attack
B. Mail bombing
C. Spoofing
D. Brute force attack

Answer: BCD

NEW QUESTION 264
- (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 269
- (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 273
- (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 278
- (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 280
- (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 283
- (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 288
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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