Actualtests.CISSP-ISSAP.237.QA

Number: CISSP-ISSAP
Passing Score: 800
Time Limit: 120 min
File Version: 26.1

ISSAP

ISSAP Information Systems Security Architecture Professional

★Our training paths will help you prepare very well for gain success in exam.

★Guaranteed 100 percent Success at this VCE with Real Questions and their Verified Answers. Get this Certification dump now.

★All the study tools available at Exam collection are great ones and I certainly did everything with perfection. I was in need of the reliable and fantastic helping stuff and thank God that you guys support and guided in the right way.

★I prepared with this practice test question and answers, which are a really good source of practice. So I learnt to manage my time and I knew the kind of questions to expect in the exam as well.

★A big success is waiting for you :) Just study it.

Sections

1. Volume A
2. Volume B

Exam A

QUESTION 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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 2
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Updated.

QUESTION 3
Which of the following is used to authenticate asymmetric keys?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: DC
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 5
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 7
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.

Correct Answer: ADE
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 8
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 9
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.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 10
Which of the following protocols uses public-key cryptography to authenticate the remote computer?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 11
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 12
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

Correct Answer: ABC
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 13
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

Correct Answer: DAC
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 14
Which of the following types of attacks cannot be prevented by technical measures only?

A. Social engineering
B. Brute force
C. Smurf DoS
D. Ping flood attack

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 15
Which of the following attacks can be overcome by applying cryptography?

A. Web ripping

B. DoS
C. Sniffing
D. Buffer overflow

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 16
Which of the following authentication methods prevents unauthorized execution of code on remote systems?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 17
The simplest form of a firewall is a packet filtering firewall. Typically a router works as a packet-filtering firewall and has the capability to filter on some of the contents of packets. On which of the following layers of the OSI reference model do these routers filter information? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: DA
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 18
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

Correct Answer: CD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 19
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. John notices that the We-are-secure network is vulnerable to a man-in-the-middle attack since the key exchange process of the cryptographic algorithm it is using does not thenticate participants. Which of the following cryptographic algorithms is being used by the We-are-secure server?

A. Blowfish
B. Twofish
C. RSA
D. Diffie-Hellman

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 20
Which of the following electrical events shows a sudden drop of power source that can cause a wide variety of problems on a PC or a network?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 21
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 22
You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 23
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

Correct Answer: CE
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 24
You work as a Network Administrator for NetTech Inc. You want to have secure communication on the company's intranet. You decide to use public key and private key pairs.
What will you implement to accomplish this?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 25
Which of the following protocols is used to compare two values calculated using the Message Digest (MD5) hashing function?

A. CHAP
B. PEAP
C. EAP
D. EAP-TLS

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 26
Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 27
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.

Correct Answer: BC
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 29
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 30
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 31
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 32
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 33
Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead-space?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 34
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 35
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 36
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 37
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

Correct Answer: BD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 38
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 39
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 40
Which of the following layers of the OSI model corresponds to the Host-to-Host layer of the TCP/IP model?

A. The transport layer
B. The presentation layer
C. The session layer

D. The application layer

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 41
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.

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 42
The ATM of a bank is robbed by breaking the ATM machine. Which of the following physical security devices can now be used for verification and historical analysis of the ATM robbery?

A. Key card
B. Biometric devices
C. Intrusion detection systems
D. CCTV Cameras

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 43
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 44
Which of the following are the countermeasures against a man-in-the-middle attack? Each correct answer represents a complete solution. Choose all that apply.

A. Using public key infrastructure authentication.
B. Using basic authentication.
C. Using Secret keys for authentication.
D. Using Off-channel verification.

Correct Answer: ACD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is an electrical event shows that there is enough power on the grid to prevent from a total power loss but there is no enough power to meet the current electrical demand?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 46
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Modified.

QUESTION 47
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.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 48
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

A.
B.
C.
D.

Correct Answer:
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 49
Which of the following should the administrator ensure during the test of a disaster recovery plan?

A. Ensure that the plan works properly
B. Ensure that all the servers in the organization are shut down.
C. Ensure that each member of the disaster recovery team is aware of their responsibility.
D. Ensure that all client computers in the organization are shut down.

Correct Answer: CA
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 50
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

Correct Answer: EBCD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 51
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 52
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

Correct Answer: BDC
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 53
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

Correct Answer: DB
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 54
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.

Correct Answer: ABD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 55
An organization is seeking to implement a hot site and wants to maintain a live database server at the backup site. Which of the following solutions will be the best for the organization?

A. Electronic vaulting
B. Remote journaling
C. Remote mirroring
D. Transaction logging

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 56
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 57
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

Correct Answer: D
Section: Volume A

Explanation

Explanation/Reference:

QUESTION 58
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 59
You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 60
A network is configured on a Bus topology. Which of the following conditions could cause a network failure? Each correct answer represents a complete solution. Choose all that apply.

A. A break in a network cable
B. 75 ohm terminators at open ends
C. A powered off workstation
D. An open-ended cable without terminators

Correct Answer: DBA
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is an input device that is used for controlling machines such as cranes, trucks, underwater unmanned vehicles, wheelchairs, surveillance cameras, and zero turning radius lawn mowers?

A. PS/2
B. Joystick
C. Microphone
D. AGP

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 62
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 63
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.

Correct Answer: CD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 64
Which of the following devices is a least expensive power protection device for filtering the electrical stream to control power surges, noise, power sags, and power spikes?

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 65
You work as a Project Manager for Tech Perfect Inc. You are creating a document which emphasizes the formal study of what your organization is doing currently and where it will be in the future. Which of the following analysis will help you in accomplishing the task?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 66
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

Correct Answer: CBA
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 67
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 68
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.

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 69
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 70
John works as a Network Administrator for NetPerfect Inc. The company has a Windows- based network. John has been assigned a project to build a network for the sales department of the company. It is important for the LAN to continue working even if there is a break in the cabling. Which of the following topologies should John use to accomplish the task?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 71
Which of the following encryption algorithms are based on block ciphers?

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

Correct Answer: DCB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 72

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 73
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. These layers reside at the top of the model.
B. Layers 4 through 7 define the functionality of IP Addressing, Physical Standards, and Data Link protocols.
C. Layers 5, 6, and 7 focus on the Network Application, which includes data formatting and session control.
D. 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.

Correct Answer: CD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 74
Which of the following is the technology of indoor or automotive environmental comfort?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 75
Which of the following protocols provides certificate-based authentication for virtual private networks (VPNs)?

A. PPTP
B. SMTP

C. HTTPS
D. L2TP

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 76
Which of the following types of ciphers are included in the historical ciphers? Each correct answer represents a complete solution. Choose two.

A. Block ciphers
B. Transposition ciphers
C. Stream ciphers
D. Substitution ciphers

Correct Answer: DB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 77
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 78
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 79
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.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 80
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.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 81
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 82
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 83
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.

Correct Answer: ACD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 84
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 85
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 86
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

Correct Answer: AB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 87
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)

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 88
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

Correct Answer: CA
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 89
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

Correct Answer: BC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 90
Fill in the blank with the appropriate security method. ____________ is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer- based information system.

A. Access control

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 91
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 92
Which of the following heights of fence deters only casual trespassers?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 93
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 94
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)

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 95
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 96
Fill in the blank with the appropriate security device. ___________ is a device that contains a physical mechanism or electronic sensor that quantifies motion that can be either integrated with or connected to other devices that alert the user of the presence of a moving object within the field of view.

A. Motion detector

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 97
Which of the following uses a Key Distribution Center (KDC) to authenticate a principle?

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 98
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 99
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 weekdays. Keep Monday's backup offsite.
C. Take a full backup daily with the previous night's tape taken offsite.
D. Take a full backup on alternate days and keep rotating the tapes.
E. Take a full backup on Monday and an incremental backup on each of the following weekdays. Keep Monday's backup offsite.
F:Take a full backup daily with one tape taken offsite weekly.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 100
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

Correct Answer: AC

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 101
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

Correct Answer: BC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 102
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 103
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)

Correct Answer: BC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 104
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

Correct Answer: AC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 105
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

Correct Answer: CBA
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 106
At which of the following layers of the Open System Interconnection (OSI) model the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP) work?

A. The Physical layer
B. The Data-Link layer
C. The Network layer
D. The Presentation layer

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 107
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

Correct Answer: CB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 108
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.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Appropriated.

QUESTION 109
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 110
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

Correct Answer: AC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 111
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

Correct Answer: BD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 112
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

Correct Answer: CB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 113
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 114
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 115

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 116
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 117
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 118
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 119
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 120
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 121
Which of the following protects against unauthorized access to confidential information via encryption and works at the network layer?

A. Firewall
B. NAT
C. MAC address
D. IPSec

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 122
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.

Correct Answer: DB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 123
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 124
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 125

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? Each correct answer represents a complete solution. Choose two.

A. MAC filtering the router
B. Not broadcasting SSID
C. Using WEP encryption
D. Using WPA encryption

Correct Answer: CD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 126
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 127
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

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 128
Which of the following uses public key cryptography to encrypt the contents of files?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 129
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

Correct Answer: DAB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 130
You are the Network Administrator for a bank. In addition to the usual security issues, you are concerned that your customers could be the victim of phishing attacks that use fake bank Web sites. Which of the following would protect against this?

A. MAC
B. Mutual authentication
C. Three factor authentication
D. Two factor authentication

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 131
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 132
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 = Asset Value (AV) * Exposure Factor (EF)
B. SLE = Asset Value (AV) * Annualized Rate of Occurrence (ARO)

C. SLE = Annualized Loss Expectancy (ALE) * Annualized Rate of Occurrence (ARO)
D. SLE = Annualized Loss Expectancy (ALE) * Exposure Factor (EF)

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 133
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

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:
Corrected.

QUESTION 134
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 135
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)

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 136
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)

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 137
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 138
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 139
Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose three.

A. It hides the internal IP addressing scheme.
B. It protects network from the password guessing attacks.
C. It is used to connect private networks to the public Internet.
D. It shares public Internet addresses with a large number of internal network clients.

Correct Answer: CAD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 140
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)

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 141
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 142
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)

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 143
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 144
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 145
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 146
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 147
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)

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Answer is renovated.

QUESTION 148
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 149
Which of the following protocols should a Chief Security Officer configure in the network of his company to protect sessionless datagram protocols?

A. SWIPE
B. S/MIME
C. SKIP
D. SLIP

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 150
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 151
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

Correct Answer: E
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 152
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

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 153
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. ElGamal

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 154
John works as an Ethical Hacker for company Inc. He wants to find out the ports that are open in company's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP FIN

B. Xmas tree
C. TCP SYN/ACK
D. TCP SYN

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 155
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 156
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 157
Which of the following categories of access controls is deployed in the organization to prevent all direct contacts with systems?

A. Detective access control
B. Physical access control
C. Technical access control
D. Administrative access control

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 158
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 159
Which of the following algorithms is found to be suitable for both digital signature and encryption?

A. SHA-1
B. MD5
C. AES
D. RSA

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 160
Which of the following is responsible for maintaining certificates in a public key infrastructure (PKI)?

A. Domain Controller
B. Certificate User
C. Certification Authority
D. Internet Authentication Server

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 161
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 162
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 163
Which of the following are used to suppress gasoline and oil fires? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: BCD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 164
Fill in the blank with the appropriate phrase. The is a simple document that provides a high- level view of the entire organization's disaster recovery efforts.

A. Executive summary

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 165
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. ccording 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.

Correct Answer: CBD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 166
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)

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Absolutely right.

QUESTION 167
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 168
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

Correct Answer: DCB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 169
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 170
Which of the following plans is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources?

A. Disaster recovery plan
B. Contingency plan
C. Business Continuity plan
D. Continuity of Operations plan

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 171
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 172
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

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 173
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

Correct Answer: CDB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 174
Which of the following authentication protocols sends a user certificate inside an encrypted tunnel?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 175
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 176
Which of the following algorithms can be used to check the integrity of a file? Each correct answer represents a complete solution. Choose two.

A. md5
B. rsa

C. blowfish
D. sha

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 177
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.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 178
The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 179
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.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 180
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 181
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 182
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 183
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 184
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Accurate Answer.

QUESTION 185
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 186
Perfect World Inc., provides its sales managers access to the company's network from remote locations. The sales managers use laptops to connect to the network. For security purposes, the company's management wants the sales managers to log on to the network using smart cards over a remote connection. Which of the following authentication protocols should be used to accomplish this?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 187
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 188
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 189
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 190
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.

Correct Answer: BCA
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 191
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 192
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

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 193
Jasmine is creating a presentation. She wants to ensure the integrity and authenticity of the presentation. Which of the following will she use to accomplish the task?

A. Mark as final
B. Digital Signature
C. Restrict Permission
D. Encrypt Document

Correct Answer: B

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 194
Which of the following elements of planning gap measures the gap between the total potential for the market and the actual current usage by all the consumers in the market?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 195
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 196
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 197
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)

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 198
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 199
Which of the following security devices is presented to indicate some feat of service, a special accomplishment, a symbol of authority granted by taking an oath, a sign of legitimate employment or student status, or as a simple means of identification?

A. Sensor
B. Alarm
C. Motion detector
D. Badge

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 200
You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering? Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption
B. Ease of maintenance
C. Failover
D. Load balancing

Correct Answer: AB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 201
Which of the following is the most secure method of authentication?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 202
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

Correct Answer: CB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 203
Which of the following cryptographic algorithm uses public key and private key to encrypt or decrypt data ?

A. Asymmetric
B. Hashing
C. Numeric
D. Symmetric

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 204
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

Correct Answer: A

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 205
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 206
You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 207
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)

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 208
Which of the following protocols provides connectionless integrity and data origin authentication of IP packets?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 209
The network you administer allows owners of objects to manage the access to those objects via access control lists. This is an example of what type of access control?

A. RBAC
B. MAC
C. CIA
D. DAC

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 210
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Renewed.

QUESTION 211
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.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 212
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 213
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

Correct Answer: ADE
Section: Volume B
Explanation

Explanation/Reference:
Still Valid.

QUESTION 214
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 215
In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

A. Initiation
B. Programming and training

C. Design
D. Evaluation and acceptance

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 216
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

Correct Answer: DA
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 217
Which of the following keys is derived from a preshared key and Extensible Authentication Protocol (EAP)?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 218
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 219
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 220
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

Correct Answer: AB
Section: Volume B
Explanation

Explanation/Reference:
Still Reliable.

QUESTION 221
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 222
You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 223
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

Correct Answer: DBA
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 224
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 225
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 226
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

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 227
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 228
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 229
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.

Correct Answer: ABD

Section: Volume A
Explanation

Explanation/Reference:

QUESTION 230
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 231
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 232
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 233
Which of the following protocols is an alternative to certificate revocation lists (CRL) and allows the authenticity of a certificate to be immediately verified?

A. RSTP

B. SKIP
C. OCSP
D. HTTP

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 234
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

Correct Answer: BA
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 235
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 236
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 237

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference: