Number: CISSP-ISSAP
Passing Score: 800
Time Limit: 120
File Version: 23.0

Exam Code: CISSP-ISSAP
Exam Name: Information Systems Security Architecture Professional

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:

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:

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:

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: D, C
Section:

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:

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:

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: A, D, E
Section:

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:

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:

QUESTION 10
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:

QUESTION 11
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:

QUESTION 12
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: B, A
Section:

QUESTION 13
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:

QUESTION 14
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:

QUESTION 15
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:

QUESTION 16
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:

QUESTION 17
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:

QUESTION 18
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: B, C, A
Section:

QUESTION 19
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: D, A, C
Section:

QUESTION 20
Which of the following types of attacks cannot be prevented by technical measures only?

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

Correct Answer: A
Section:

QUESTION 21
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:

QUESTION 22
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:

QUESTION 23
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: D, A
Section:

QUESTION 24
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: C, D
Section:

QUESTION 25
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:

QUESTION 26
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:

QUESTION 27
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:

QUESTION 28
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:

QUESTION 29
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: E, C
Section:

QUESTION 30
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:

QUESTION 31
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:

QUESTION 32
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:

QUESTION 33
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: B, C
Section:

QUESTION 34
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:

QUESTION 35
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:

QUESTION 36
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:

QUESTION 37
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:

QUESTION 38
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:

QUESTION 39
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:

QUESTION 40
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:

QUESTION 41
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: D, A
Section:

QUESTION 42
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:

QUESTION 43
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:

QUESTION 44
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:

QUESTION 45
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: D, C
Section:

QUESTION 46
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:

QUESTION 47
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:

QUESTION 48
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: D, B
Section:

QUESTION 49
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 costeffective 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:

QUESTION 50
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:

QUESTION 51
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:

QUESTION 52
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:

QUESTION 53
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:

QUESTION 54
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:

QUESTION 55
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: C, A, D
Section:

QUESTION 56
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:

QUESTION 57
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:

QUESTION 58
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: D, A
Section:

QUESTION 59
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:

QUESTION 60
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:

QUESTION 61
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:

QUESTION 62
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: B, A
Section:

QUESTION 63
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:

QUESTION 64
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: B, A
Section:

QUESTION 65
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: A, D
Section:

QUESTION 66
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: C, A
Section:

QUESTION 67
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: B, C
Section:

QUESTION 68
SIMULATION 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:

QUESTION 69
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:

QUESTION 70
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:

QUESTION 71
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:

QUESTION 72
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:

QUESTION 73
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:

QUESTION 74
SIMILATION
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:

QUESTION 75
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:

QUESTION 76
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:

QUESTION 77
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:

QUESTION 78
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: A, C
Section:

QUESTION 79
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: B, C
Section:

QUESTION 80
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:

QUESTION 81
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: B, C
Section:

QUESTION 82
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: A, C
Section:

QUESTION 83
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: C, B, A
Section:

QUESTION 84
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:

QUESTION 85
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: C, B
Section:

QUESTION 86
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:

QUESTION 87
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:

QUESTION 88
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: A, C
Section:

QUESTION 89
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: B, D
Section:

QUESTION 90
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: C, B
Section:

QUESTION 91
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:

QUESTION 92
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:

QUESTION 93
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:

QUESTION 94
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:

QUESTION 95
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:

QUESTION 96
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:

QUESTION 97
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:

QUESTION 98
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:

QUESTION 99
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:

QUESTION 100
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: D, B
Section:

QUESTION 101
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:

QUESTION 102
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:

QUESTION 103
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:

QUESTION 104
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: A, D, E
Section:

QUESTION 105
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:

QUESTION 106
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:

QUESTION 107
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:

QUESTION 108
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:

QUESTION 109
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: D, C, B
Section:

QUESTION 110
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:

QUESTION 111
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:

QUESTION 112
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:

QUESTION 113
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: A, B, D
Section:

QUESTION 114
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: C, D, B
Section:

QUESTION 115
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:

QUESTION 116
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:

QUESTION 117
Which of the following algorithms can be used to check the integrity of a file? 158
Each correct answer represents a complete solution. Choose two.

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

Correct Answer: A, D
Section:

QUESTION 118
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:

QUESTION 119
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:

QUESTION 120
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:

QUESTION 121
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:

QUESTION 122
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:

QUESTION 123
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:

QUESTION 124
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:

QUESTION 125
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:

QUESTION 126
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:

QUESTION 127
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:

QUESTION 128
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:

QUESTION 129
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:

QUESTION 130
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: B, A
Section:

QUESTION 131
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:

QUESTION 132
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: C, B
Section:

QUESTION 133
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: