ISC2

Exam Questions ISSAP

ISSAP Information Systems Security Architecture Professional

NEW QUESTION 1
- (Exam Topic 1)
Which of the following statements about a stream cipher are true? Each correct answer represents a complete solution. Choose three.

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

Answer: ADE

NEW QUESTION 2
- (Exam Topic 1)
A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

A. Denial-of-Service attack
B. Vulnerability attack
C. Social Engineering attack
D. Impersonation attack

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

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

Answer: C

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

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

Answer: ABD

NEW QUESTION 5
- (Exam Topic 1)
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)

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Which of the following types of attack can be used to break the best physical and logical security mechanism to gain access to a system?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
Andrew works as a Network Administrator for Infonet Inc. The company's network has a Web server that hosts the company's Web site. Andrew wants to increase the security of the Web site by implementing Secure Sockets Layer (SSL). Which of the following types of encryption does SSL use? Each correct answer represents a complete solution. Choose two.

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

Answer: CD

NEW QUESTION 8
- (Exam Topic 1)
IPsec VPN provides a high degree of data privacy by establishing trust points between communicating devices and data encryption. Which of the following encryption methods does IPsec VPN use? Each correct answer represents a complete solution. Choose two.

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

Answer: CD

NEW QUESTION 9
- (Exam Topic 1)
You are the Network Administrator for a small business. You need a widely used, but highly secure hashing algorithm. Which of the following should you choose?

A. AES
B. SHA
C. EAP
D. CRC32

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 13
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 17
- (Exam Topic 1)
You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

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

Answer: A

NEW QUESTION 22
- (Exam Topic 1)
Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

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

Answer: B

NEW QUESTION 27
- (Exam Topic 1)
In which of the following network topologies does the data travel around a loop in a single direction and pass through each device?

A. Ring topology
B. Tree topology
C. Star topology
D. Mesh topology

Answer: A

NEW QUESTION 29
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 33
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 37
- (Exam Topic 1)
Which of the following statements about incremental backup are true? Each correct answer represents a complete solution. Choose two.

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

Answer: AD

NEW QUESTION 42
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 47
- (Exam Topic 1)
Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

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

Answer: D

NEW QUESTION 52
- (Exam Topic 2)
Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

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

Answer: A

NEW QUESTION 55
- (Exam Topic 2)
You work as an administrator for Techraft Inc. Employees of your company create 'products', which are supposed to be given different levels of access. You need to configure a security policy in such a way that an employee (producer of the product) grants accessing privileges (such as read, write, or alter) for his product. Which of the following access control models will you use to accomplish this task?

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

Answer: A

NEW QUESTION 56
- (Exam Topic 2)
Your customer is concerned about security. He wants to make certain no one in the outside world can see the IP addresses inside his network. What feature of a router would accomplish this?

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

Answer: B

NEW QUESTION 61
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 66
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 68
- (Exam Topic 2)
You are the administrator for YupNo.com. You want to increase and enhance the security of your computers and simplify deployment. You are especially concerned with any portable computers that are used by remote employees. What can you use to increase security, while still allowing your users to perform critical tasks?

A. BitLocker
B. Smart Cards
C. Service Accounts
D. AppLocker

Answer: B

NEW QUESTION 73
- (Exam Topic 2)
Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

A. SLE = 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)

Answer: A

NEW QUESTION 75
- (Exam Topic 2)
You work as a Chief Security Officer for Tech Perfect Inc. The company has an internal room without any window and is totally in darkness. For security reasons, you want to place a device in the room. Which of the following devices is best for that room?

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

Answer: A

NEW QUESTION 76
- (Exam Topic 2)
Which of the following backup types backs up files that have been added and all data that have been modified since the most recent backup was performed?

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

Answer: B

NEW QUESTION 77
- (Exam Topic 2)
Which of the following protocols work at the Network layer of the OSI model?

A. Routing Information Protocol (RIP)
B. File Transfer Protocol (FTP)
C. Simple Network Management Protocol (SNMP)
D. Internet Group Management Protocol (IGMP)

Answer: AD

NEW QUESTION 82
- (Exam Topic 2)
You work as a Network Administrator for Net World Inc. You are required to configure a VLAN for the company. Which of the following devices will you use to physically connect the computers in the VLAN? Each correct answer represents a complete solution. Choose two.

A. Switch
B. Router
C. Bridge
D. Hub
E. Repeater

Answer: AB

NEW QUESTION 85
- (Exam Topic 2)
Which of the following are the phases of the Certification and Accreditation (C&A) process? Each correct answer represents a complete solution. Choose two.

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

Answer: BC

NEW QUESTION 89
- (Exam Topic 2)
You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You have a disaster scenario and you want to discuss it with your team members for getting

appropriate responses of the disaster. In which of the following disaster recovery tests can this task be performed?

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

Answer: C

NEW QUESTION 91
- (Exam Topic 2)
Which of the following algorithms can be used to check the integrity of a file? 158
Each correct answer represents a complete solution. Choose two.

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

Answer: AD

NEW QUESTION 92
- (Exam Topic 2)
You are implementing some security services in an organization, such as smart cards, biometrics, access control lists, firewalls, intrusion detection systems, and clipping levels. Which of the following categories of implementation of the access control includes all these security services?

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

Answer: B

NEW QUESTION 95
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 97
- (Exam Topic 2)
Which of the following authentication methods is based on physical appearance of a user?

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

Answer: B

NEW QUESTION 98
- (Exam Topic 2)
You are the Network Administrator at a large company. Your company has a lot of contractors and other outside parties that come in and out of the building. For this reason you are concerned that simply having usernames and passwords is not enough and want to have employees use tokens for authentication. Which of the following is not an example of tokens?

A. Smart card
B. USB device with cryptographic data
C. CHAP
D. Key fob

Answer: C

NEW QUESTION 102
- (Exam Topic 2)
Which of the following components come under the network layer of the OSI model? Each correct answer represents a complete solution. Choose two.

A. Routers
B. MAC addresses
C. Firewalls
D. Hub

Answer: AC

NEW QUESTION 103
- (Exam Topic 2)
Which of the following uses public key cryptography to encrypt the contents of files?

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

Answer: A

NEW QUESTION 107
- (Exam Topic 2)
In which of the following SDLC phases are the software and other components of the system faithfully incorporated into the design specifications?

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

Answer: A

NEW QUESTION 108
- (Exam Topic 2)
Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Eradication phase
B. Recovery phase
C. Containment phase
D. Preparation phase
E. Identification phase

Answer: D

NEW QUESTION 112
- (Exam Topic 2)
You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

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

Answer: C

NEW QUESTION 114
- (Exam Topic 2)
You are responsible for security at a building that has a lot of traffic. There are even a significant number of non-employees coming in and out of the building. You are concerned about being able to find out who is in the building at a particular time. What is the simplest way to accomplish this?

A. Implement a sign in sheet at the main entrance and route all traffic through there.
B. Have all people entering the building use smart cards for access.
C. Implement biometric access.
D. Implement cameras at all entrances.

Answer: A

NEW QUESTION 119
- (Exam Topic 2)
Which of the following authentication protocols sends a user certificate inside an encrypted tunnel?

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

Answer: B

NEW QUESTION 122
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 126
- (Exam Topic 2)
Which of the following uses a Key Distribution Center (KDC) to authenticate a principle?

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

Answer: C

NEW QUESTION 127
- (Exam Topic 2)
Which of the following security protocols provides confidentiality, integrity, and authentication of network traffic with end-to-end and intermediate-hop security?

A. IPSec
B. SET
C. SWIPE
D. SKIP

Answer: C

NEW QUESTION 132
- (Exam Topic 2)
Della works as a security manager for SoftTech Inc. She is training some of the newly recruited personnel in the field of security management. She is giving a tutorial on DRP. She explains that the major goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited personnel in SoftTech Inc, what will be your answer for her question? Each correct answer represents a part of the solution. Choose three.

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

Answer: ABC

NEW QUESTION 137
- (Exam Topic 2)
You work as a Network Administrator for McNeil Inc. The company has a TCP/IP-based network. Performance of the network is slow because of heavy traffic. A hub is used as a central connecting device in the network. Which of the following devices can be used in place of a hub to control the network traffic efficiently?

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

Answer: C

NEW QUESTION 142
- (Exam Topic 2)
You work as a Network Administrator for McRoberts Inc. You are expanding your company's network. After you have implemented the network, you test the connectivity to a remote host by using the PING command. You get the ICMP echo reply message from the remote host. Which of the following layers of the OSI model are tested through this process? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

NEW QUESTION 143
- (Exam Topic 2)
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

Answer: BD

NEW QUESTION 145
- (Exam Topic 2)
The security controls that are implemented to manage physical security are divided in various groups. Which of the following services are offered by the administrative physical security control group? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: ABCF

NEW QUESTION 146
- (Exam Topic 2)
You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 151
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 152
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

ISSAP Practice Exam Features:

* ISSAP Questions and Answers Updated Frequently

* ISSAP Practice Questions Verified by Expert Senior Certified Staff

* ISSAP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* ISSAP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year