



# ISC2

## Exam Questions ISSAP

ISSAP Information Systems Security Architecture Professional

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

- (Exam Topic 1)

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

**Answer:** ABC

#### NEW QUESTION 2

- (Exam Topic 1)

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

**Answer:** A

#### NEW QUESTION 3

- (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 4

- (Exam Topic 1)

Which of the following terms refers to the method that allows or restricts specific types of packets from crossing over the firewall?

- A. Hacking
- B. Packet filtering
- C. Web caching
- D. Spoofing

**Answer:** B

#### NEW QUESTION 5

- (Exam Topic 1)

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

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

**Answer:** BD

#### NEW QUESTION 6

- (Exam Topic 1)

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.

**Answer:** AC

#### NEW QUESTION 7

- (Exam Topic 1)

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.

**Answer:** ACD

#### NEW QUESTION 8

- (Exam Topic 1)

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

**Answer:** C

#### NEW QUESTION 9

- (Exam Topic 1)

Which of the following types of firewall functions at the Session layer of OSI model?

- A. Circuit-level firewall
- B. Application-level firewall
- C. Packet filtering firewall
- D. Switch-level firewall

**Answer:** A

#### NEW QUESTION 10

- (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 10

- (Exam Topic 1)

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

**Answer:** A

#### NEW QUESTION 11

- (Exam Topic 1)

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

**Answer:** A

#### NEW QUESTION 14

- (Exam Topic 1)

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

**Answer:** A

#### NEW QUESTION 19

- (Exam Topic 1)

Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the

disaster recovery plan?

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

**Answer:** C

#### NEW QUESTION 21

- (Exam Topic 1)

A digital signature is a type of public key cryptography. Which of the following statements are true about digital signatures? Each correct answer represents a complete solution. Choose all that apply.

- A. In order to digitally sign an electronic record, a person must use his/her public key.
- B. In order to verify a digital signature, the signer's private key must be used.
- C. In order to digitally sign an electronic record, a person must use his/her private key.
- D. In order to verify a digital signature, the signer's public key must be used.

**Answer:** CD

#### NEW QUESTION 24

- (Exam Topic 1)

Which of the following refers to a location away from the computer center where document copies and backup media are kept?

- A. Storage Area network
- B. Off-site storage
- C. On-site storage
- D. Network attached storage

**Answer:** B

#### NEW QUESTION 29

- (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 30

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 33

- (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 35

- (Exam Topic 1)

In your office, you are building a new wireless network that contains Windows 2003 servers. To establish a network for secure communication, you have to implement IPSec security policy on the servers. What authentication methods can you use for this implementation? Each correct answer represents a complete solution. Choose all that apply.

- A. Public-key cryptography
- B. Kerberos
- C. Preshared keys
- D. Digital certificates

**Answer:** BCD

**NEW QUESTION 36**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 39**

- (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 44**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 47**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 48**

- (Exam Topic 1)

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

**Answer:** D

**NEW QUESTION 52**

- (Exam Topic 1)

Which of the following encryption methods does the SSL protocol use in order to provide communication privacy, authentication, and message integrity? Each correct answer represents a part of the solution. Choose two.

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

**Answer:** AD

**NEW QUESTION 57**

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 59

- (Exam Topic 1)

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

**Answer:** C

#### NEW QUESTION 60

- (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 61

- (Exam Topic 1)

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

**Answer:** C

#### NEW QUESTION 65

- (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 69

- (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](http://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 71

- (Exam Topic 1)

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

- A. Microsoft Internet Information Server (IIS)

- B. VPN
- C. FTP server
- D. Certificate server

**Answer:** D

#### NEW QUESTION 75

- (Exam Topic 1)

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

**Answer:** C

#### NEW QUESTION 77

- (Exam Topic 1)

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

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 1)

Which of the following encryption modes can make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way?

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

**Answer:** D

#### NEW QUESTION 80

- (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 83

- (Exam Topic 1)

Which of the following two components does Kerberos Key Distribution Center (KDC) consist of? Each correct answer represents a complete solution. Choose two.

- A. Data service
- B. Ticket-granting service
- C. Account service
- D. Authentication service

**Answer:** BD

#### NEW QUESTION 86

- (Exam Topic 1)

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

**Answer:** B



#### NEW QUESTION 88

- (Exam Topic 1)

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

**Answer:** B

#### NEW QUESTION 89

- (Exam Topic 1)

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

- A. Mutual
- B. Anonymous
- C. Multi-factor
- D. Biometrics

**Answer:** C

#### NEW QUESTION 90

- (Exam Topic 1)

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

**Answer:** C

#### NEW QUESTION 91

- (Exam Topic 1)

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.

**Answer:** B

#### NEW QUESTION 96

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 97

- (Exam Topic 1)

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

**Answer:** C

#### NEW QUESTION 99

- (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 102

- (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 107

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 111

- (Exam Topic 2)

Which of the following authentication methods provides credentials that are only valid during a single session?

- A. Kerberos v5
- B. Smart card
- C. Certificate
- D. Token

**Answer:** D

#### NEW QUESTION 115

- (Exam Topic 2)

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

**Answer:** AB

#### NEW QUESTION 117

- (Exam Topic 2)

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. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Executive summary

#### NEW QUESTION 120

- (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 122

- (Exam Topic 2)

Which of the following user authentications are supported by the SSH-1 protocol but not by the SSH-2 protocol? Each correct answer represents a complete solution. Choose all that apply.

- A. TIS authentication
- B. Rhosts (rsh-style) authentication
- C. Kerberos authentication
- D. Password-based authentication

**Answer:** ABC

#### NEW QUESTION 124

- (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 125

- (Exam Topic 2)

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

**Answer:** B

#### NEW QUESTION 127

- (Exam Topic 2)

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

**Answer:** A

#### NEW QUESTION 129

- (Exam Topic 2)

Which of the following keys are included in a certificate revocation list (CRL) of a public key infrastructure (PKI)? Each correct answer represents a complete solution. Choose two.

- A. A foreign key
- B. A private key
- C. A public key
- D. A primary key

**Answer:** BC

#### NEW QUESTION 130

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 132

- (Exam Topic 2)

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

- A. Service-oriented logical design modeling

- B. Service-oriented conceptual architecture modeling
- C. Service-oriented discovery and analysis modeling
- D. Service-oriented business integration modeling

**Answer:** A

#### NEW QUESTION 134

- (Exam Topic 2)

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

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

**Answer:** BCD

#### NEW QUESTION 135

- (Exam Topic 2)

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Annualized Rate of Occurrence (ARO)
- C. Single Loss Expectancy (SLE)
- D. Exposure Factor (EF)

**Answer:** B

#### NEW QUESTION 136

- (Exam Topic 2)

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

**Answer:** A

#### NEW QUESTION 138

- (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 141

- (Exam Topic 2)

Which of the following methods of encryption uses a single key to encrypt and decrypt data?

- A. Asymmetric
- B. Symmetric
- C. S/MIME
- D. PGP

**Answer:** B

#### NEW QUESTION 145

- (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 150

- (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 152

- (Exam Topic 2)

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

Which of the following should you choose for this client?

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

**Answer:** C

#### NEW QUESTION 155

- (Exam Topic 2)

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

**Answer:** D

#### NEW QUESTION 157

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 162

- (Exam Topic 2)

Which of the following attacks allows the bypassing of access control lists on servers or routers, and helps an attacker to hide? Each correct answer represents a complete solution. Choose two.

- A. DNS cache poisoning
- B. MAC spoofing
- C. IP spoofing attack
- D. DDoS attack

**Answer:** BC

#### NEW QUESTION 163

- (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 165

- (Exam Topic 2)

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

authentication. Which of the following authentication methods will you suggest?

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

**Answer:** D

#### NEW QUESTION 170

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 173

- (Exam Topic 2)

Which of the following techniques can be used by an administrator while working with the symmetric encryption cryptography? Each correct answer represents a complete solution. Choose all that apply.

- A. Block cipher
- B. Stream cipher
- C. Transposition cipher
- D. Message Authentication Code

**Answer:** ABD

#### NEW QUESTION 177

- (Exam Topic 2)

You work as a Network Administrator for NetTech Inc. When you enter <http://66.111.64.227> in the browser 's address bar, you are able to access the site. But, you are unable to access the site when you enter <http://www.company.com>. What is the most likely cause?

- A. The site's Web server is offline.
- B. The site's Web server has heavy traffic.
- C. WINS server has no NetBIOS name entry for the server.
- D. DNS entry is not available for the host name.

**Answer:** D

#### NEW QUESTION 182

- (Exam Topic 2)

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

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

**Answer:** BC

#### NEW QUESTION 187

- (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 192

- (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 195**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 198**

- (Exam Topic 2)

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

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

**Answer:** ADEF

**NEW QUESTION 199**

- (Exam Topic 2)

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

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

**Answer:** BC

**NEW QUESTION 201**

- (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 205**

- (Exam Topic 2)

Which of the following are man-made threats that an organization faces? Each correct answer represents a complete solution. Choose three.

- A. Theft
- B. Employee errors
- C. Strikes
- D. Frauds

**Answer:** ABD

**NEW QUESTION 206**

- (Exam Topic 2)

Which of the following ports must be opened on the firewall for the VPN connection using Point-to-Point Tunneling Protocol (PPTP)?

- A. TCP port 110
- B. TCP port 443
- C. TCP port 5060
- D. TCP port 1723

**Answer:** D

**NEW QUESTION 208**

- (Exam Topic 2)



Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transfer
- D. Risk mitigation

**Answer:** C

#### NEW QUESTION 210

- (Exam Topic 2)

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

**Answer:** C

#### NEW QUESTION 213

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 215

- (Exam Topic 2)

You are calculating the Annualized Loss Expectancy (ALE) using the following formula:  $ALE = AV * EF * ARO$  What information does the AV (Asset Value) convey?

- A. It represents how many times per year a specific threat occurs.
- B. It represents the percentage of loss that an asset experiences if an anticipated threat occurs.
- C. It is expected loss for an asset due to a risk over a one year period.
- D. It represents the total cost of an asset, including the purchase price, recurring maintenance, expenses, and all other costs.

**Answer:** D

#### NEW QUESTION 219

- (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 222

- (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 226

- (Exam Topic 2)

You work as a Security Manager for Tech Perfect Inc. The management tells you to implement a hashing method in the organization that can resist forgery and is not open to the man-in-the-middle attack. Which of the following methods will you use to accomplish the task?

- A. MD
- B. NTLM
- C. MAC
- D. SHA



**Answer:** C

#### NEW QUESTION 228

- (Exam Topic 2)

Which of the following methods will allow data to be sent on the Internet in a secure format?

- A. Serial Line Interface Protocol
- B. Point-to-Point Protocol
- C. Browsing
- D. Virtual Private Networks

**Answer:** D

#### NEW QUESTION 233

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 234

- (Exam Topic 2)

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

**Answer:** D

#### NEW QUESTION 239

- (Exam Topic 2)

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

**Answer:** D

#### NEW QUESTION 240

- (Exam Topic 2)

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

**Answer:** C

#### NEW QUESTION 242

- (Exam Topic 2)

The OSI model is the most common networking model used in the industry. Applications, network functions, and protocols are typically referenced using one or more of the seven OSI layers. Of the following, choose the two best statements that describe the OSI layer functions. Each correct answer represents a complete solution. Choose two.

- A. Layers 1 and 2 deal with application functionality and data formatting.
- B. These layers reside at the top of the model.
- C. Layers 4 through 7 define the functionality of IP Addressing, Physical Standards, and Data Link protocols.
- D. Layers 5, 6, and 7 focus on the Network Application, which includes data formatting and session control.
- E. Layers 1, 2, 3, and 4 deal with physical connectivity, encapsulation, IP Addressing, and Error Recovery. These layers define the end-to-end functions of data delivery.

**Answer:** CD

#### NEW QUESTION 244

- (Exam Topic 2)

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

- A. Parallel test
- B. Simulation test
- C. Full-interruption test
- D. Checklist test

**Answer:** D

#### NEW QUESTION 245

- (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 248

- (Exam Topic 2)

You work as a remote support technician. A user named Rick calls you for support. Rick wants to connect his LAN connection to the Internet. Which of the following devices will you suggest that he use?

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

**Answer:** E

#### NEW QUESTION 251

- (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 253

- (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 256

- (Exam Topic 2)

Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation

- A. Design
- B. Maintenance
- C. Deployment
- D. Requirements Gathering

**Answer:** A

#### NEW QUESTION 260

- (Exam Topic 2)

You work as a Chief Security Officer for Tech Perfect Inc. The company has a TCP/IP based network. You want to use a firewall that can track the state of active connections of the network and then determine which network packets are allowed to enter through the firewall. Which of the following firewalls has this feature?

- A. Stateful packet inspection firewall
- B. Proxy-based firewall

- C. Dynamic packet-filtering firewall
- D. Application gateway firewall

**Answer:** C

#### NEW QUESTION 265

- (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 270

- (Exam Topic 2)

Which of the following schemes is used by the Kerberos authentication?

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

**Answer:** C

#### NEW QUESTION 271

- (Exam Topic 2)

Which of the following are used to suppress electrical and computer fires? Each correct answer represents a complete solution. Choose two.

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

**Answer:** AC

#### NEW QUESTION 276

- (Exam Topic 2)

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

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

**Answer:** ABD

#### NEW QUESTION 277

- (Exam Topic 2)

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. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Motion detector

#### NEW QUESTION 280

- (Exam Topic 2)

Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

- A. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer
- B. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer
- C. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer
- D. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

**Answer:** D

#### NEW QUESTION 284

- (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 286

- (Exam Topic 2)

Which of the following is a network service that stores and organizes information about a network users and network resources and that allows administrators to manage users' access to the resources?

- A. SMTP service
- B. Terminal service
- C. Directory service
- D. DFS service

**Answer:** C

#### NEW QUESTION 290

- (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 294

.....

## Relate Links

**100% Pass Your ISSAP Exam with Examible Prep Materials**

<https://www.examible.com/ISSAP-exam/>

## Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste - <https://www.examible.com/>**