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 protocols multicasts messages and information among all member devices in an IP multicast group?

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

Answer: D

NEW QUESTION 3
- (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 4
- (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 5
- (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 6
- (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 7
- (Exam Topic 1)
Which of the following statements best describes a certification authority?

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

D. A certification authority is a type of encryption that uses a single key to encrypt and decrypt data.

Answer: C

NEW QUESTION 8
- (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 9
- (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)
You work as a technician for Trade Well Inc. The company is in the business of share trading. To enhance security, the company wants users to provide a third key (apart from ID and password) to access the company's Web site. Which of the following technologies will you implement to accomplish the task?

A. Smart cards
B. Key fobs
C. VPN
D. Biometrics

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Which of the following layers of the OSI model corresponds to the Host-to-Host layer of the TCP/IP model?

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

Answer: A

NEW QUESTION 11
- (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 14
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 15
- (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 19
- (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 21
- (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 26
- (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 30
- (Exam Topic 1)
Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme? Each correct answer represents a complete solution. Choose all that apply.

A. Kerberos requires continuous availability of a central server.
B. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's passwords.
C. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.
D. Kerberos requires the clocks of the involved hosts to be synchronized.

Answer: ABD

NEW QUESTION 34
- (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 35
- (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 37
- (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 38
- (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 39
- (Exam Topic 2)
You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

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

Answer: A

NEW QUESTION 44
- (Exam Topic 2)
You work as a Chief Security Officer for Tech Perfect Inc. You have configured IPSec and ISAKMP protocol in the company's network in order to establish a secure communication infrastructure. ccording to the Internet RFC 2408, which of the following services does the ISAKMP protocol offer to the network? Each correct answer represents a part of the solution. Choose all that apply.

A. It relies upon a system of security associations.
B. It provides key generation mechanisms.
C. It authenticates communicating peers.
D. It protects against threats, such as DoS attack, replay attack, etc.

Answer: BCD

NEW QUESTION 47
- (Exam Topic 2)
Which of the following protocols supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection?

A. PPTP
B. UDP
C. IPSec
D. PAP

Answer: A

NEW QUESTION 51
- (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 56
- (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 57
- (Exam Topic 2)
You work as a Security Manager for Tech Perfect Inc. A number of people are involved with you in the DRP efforts. You have maintained several different types of plan documents, intended for different audiences. Which of the following documents will be useful for you as well as public relations personnel who require a non-technical perspective on the entire organization's disaster recovery efforts?

A. Technical guide
B. Executive summary
C. Checklist
D. Department-specific plan

Answer: B

NEW QUESTION 59
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 63
- (Exam Topic 2)
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.

Answer: ACD

NEW QUESTION 68
- (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 69
- (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 70
- (Exam Topic 2)

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

A. Disaster recovery plan
B. Contingency plan
C. Business continuity plan
D. Crisis communication plan

Answer: C

NEW QUESTION 75
- (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 76
- (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 80
- (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 85
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 88
- (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 89
- (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 94
- (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 99
- (Exam Topic 2)
Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

A. Kerberos
B. Cryptography
C. Cryptographer
D. Cryptanalysis

Answer: D

NEW QUESTION 101
- (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 103
- (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 107
- (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 108
- (Exam Topic 2)
John works as an Ethical Hacker for company Inc. He wants to find out the ports that are open in company's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

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

Answer: D

NEW QUESTION 111
- (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 113
- (Exam Topic 2)
Which of the following are types of asymmetric encryption algorithms? Each correct answer represents a complete solution. Choose two.

A. RSA
B. AES
C. ECC
D. DES

Answer: AC

NEW QUESTION 115
- (Exam Topic 2)
Which of the following statements are true about Public-key cryptography? Each correct answer represents a complete solution. Choose two.

A. Data encrypted with the secret key can only be decrypted by another secret key.
B. The secret key can encrypt a message, and anyone with the public key can decrypt it.
C. The distinguishing technique used in public key-private key cryptography is the use of symmetric key algorithms.
D. Data encrypted by the public key can only be decrypted by the secret key.

Answer: BD

NEW QUESTION 119
- (Exam Topic 2)
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. Mastered
B. Not Mastered

Answer: A

Explanation:
Access control

NEW QUESTION 124
- (Exam Topic 2)
Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

A. Spoofing
B. Packet sniffing
C. Tunneling
D. Packet filtering

Answer: C

NEW QUESTION 126
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 127
- (Exam Topic 2)
Which of the following are types of access control attacks? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 130
- (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 131
- (Exam Topic 2)
Adam works as a Network Administrator. He discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. Which of the following types of authentication mechanism is used here?

A. Pre-shared key authentication
B. Open system authentication
C. Shared key authentication
D. Single key authentication

Answer: C

NEW QUESTION 132
- (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 133
- (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 138
- (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 143
- (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 144

......

Relate Links

100% Pass Your ISSAP Exam with Exambible Prep Materials

https://www.exambible.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.exambible.com/