Free Questions for ISSAP by certsdeals

Shared by Wallace on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- Disaster recovery plan

B- Contingency plan

C- Business Continuity plan

D- Continuity of Operations plan

Answer:

A

Explanation:

considerable loss of information systems resources. The chief objective of a disaster recovery plan is to provide an organized way to make

decisions if a disruptive event occurs.

Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption

of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes

planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the

disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.

Answer option C is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an

organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster

or extended disruption. The logistical plan is called a business continuity plan.

Answer option D is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United

States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any

period where normal operations are unattainable.

Answer option B is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are

often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific

strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also

include a monitoring process and 'triggers' for initiating planned actions. They are required to help governments, businesses, or individuals to

recover from serious incidents in the minimum time with minimum cost and disruption.

Question 2

Question Type: MultipleChoice

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

Options:

A- TCP port 110

B- TCP port 443

C- TCP port 5060

D- TCP port 1723

Answer:

D

Explanation:

(PPTP) .

Point-to-Point Tunneling Protocol (PPTP) is a remote access protocol. It is an extension of the Point-to-Point Protocol (PPP). PPTP is used to

securely connect to a private network by a remote client using a public data network, such as the Internet. Virtual private networks (VPNs)

use the tunneling protocol to enable remote users to access corporate networks securely across the Internet. PPTP supports encapsulation of

encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection.

Answer option B is incorrect. Secure Sockets Layer (SSL) uses TCP port 443 as the default port.

Answer option C is incorrect. TCP/UDP port 5060 is used for the Session Initiation Protocol (SIP).

Answer option A is incorrect. TCP port 110 is the default port for POP3.

Question 3

Question Type: **MultipleChoice**

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.

Options:

A- Identification

B- Eradication

C- Recovery

D- Contamination

E- Preparation

Answer:

B, C, D

Explanation:

process is responsible for supporting and building up the incident combating process. It ensures the stability of the system and also confirms

that the incident does not get any worse. The Containment phase includes the process of preventing further contamination of the system or

network, and preserving the evidence of the contamination.

The loss done to the system due to spamming is recovered using the recovery phase. The Recovery phase of the Incident handling process is

the stage at which the enterprise or the system is settled back to its balanced production state. It involves the quality assurance tests and

re-evaluation of the system for the purpose of the system revival or recovery.

The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes

the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from

happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied.

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- Certification Practice Statement

B- Certificate Policy

C- Certificate Revocation List

D- Certification Authority

Answer:

C

Explanation:

longer valid, and therefore should not be relied upon. A CRL is generated and published periodically, after a defined timeframe. A CRL can also

be published immediately after a certificate has been revoked. The CRL is always issued by the CA which issues the corresponding certificates.

All CRLs have a lifetime during which they are valid; this timeframe is often 24 hours or less. During a CRL's validity period, it may be consulted

by a PKI-enabled application to verify a certificate prior to use.

Answer option A is incorrect. A certification Practice Statement (CPS) is a policy document, defined by the American Bar Association. The CPS is

associated with a certification authority (CA). It defines the measures that are used to secure CA operations and management of the

certificates issued by the CA. The CPS can be considered as an agreement between the organization managing the CA and the people relying on the certificates issued by the CA.

Answer option B is incorrect. Certificate Policy is a policy statement defined in the X.509 standard. The CP is associated with a certificate. It defines the measures that are used to validate a certificate's subject prior to certificate issuance and the CA's responsibilities regarding those certificates. The CP is also considered as the certificate-issuance policy which can determine whether the presented certificate will be trusted or not.

Answer option D is incorrect. A certification authority (CA) or certificate authority is an entity that issues digital certificates for use by other parties. It is an example of a trusted third party. A CA issues digital certificates that contain a public key and the identity of the owner. The matching private key is not similarly made available publicly, but kept secret by the end user who generated the key pair. The certificate is also an attestation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. A variety of standards and tests are used by CAs to do so.

If the user trusts the CA and can verify the CA's signature, then he can also verify that a certain public key does indeed belong to a person

identified in the certificate.

Question 5

Question Type: **MultipleChoice**

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?

Options:

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

Explanation:

software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems.

The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling

practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling

framework illustrates the major elements that identify the 'what to do' aspects of a service development scheme.

Answer option D is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems

development and integration.

Answer option B is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends

traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA.

Answer option C is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security

Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures

and for delivering security infrastructure solutions that support critical business initiatives.

Question 6

Question Type: **MultipleChoice**

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.

Options:

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:

B, C, D

Explanation:

It authenticates communicating peers.

It creates and manages security associations.

It provides key generation mechanisms.

It protects against threats, such as DoS attack, replay attack, etc.

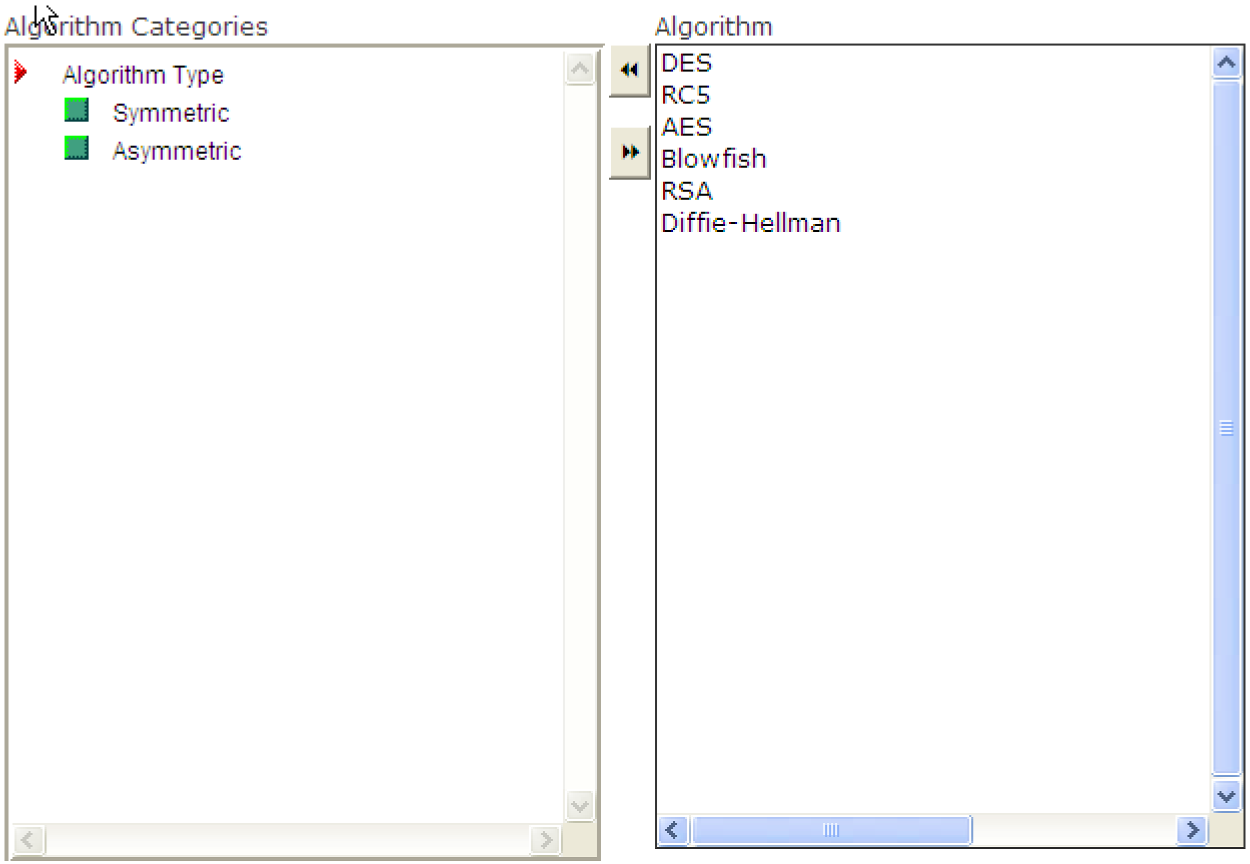
Answer option A is incorrect. The ISAKMP protocol does not relies upon a system of security association. This service is offered by the IPSec

protocol. The ISAKMP only manages these security associations.

Question 7

Question Type: MultipleChoice

Place the encryption algorithms in their respective categories.



Algorithm Categories

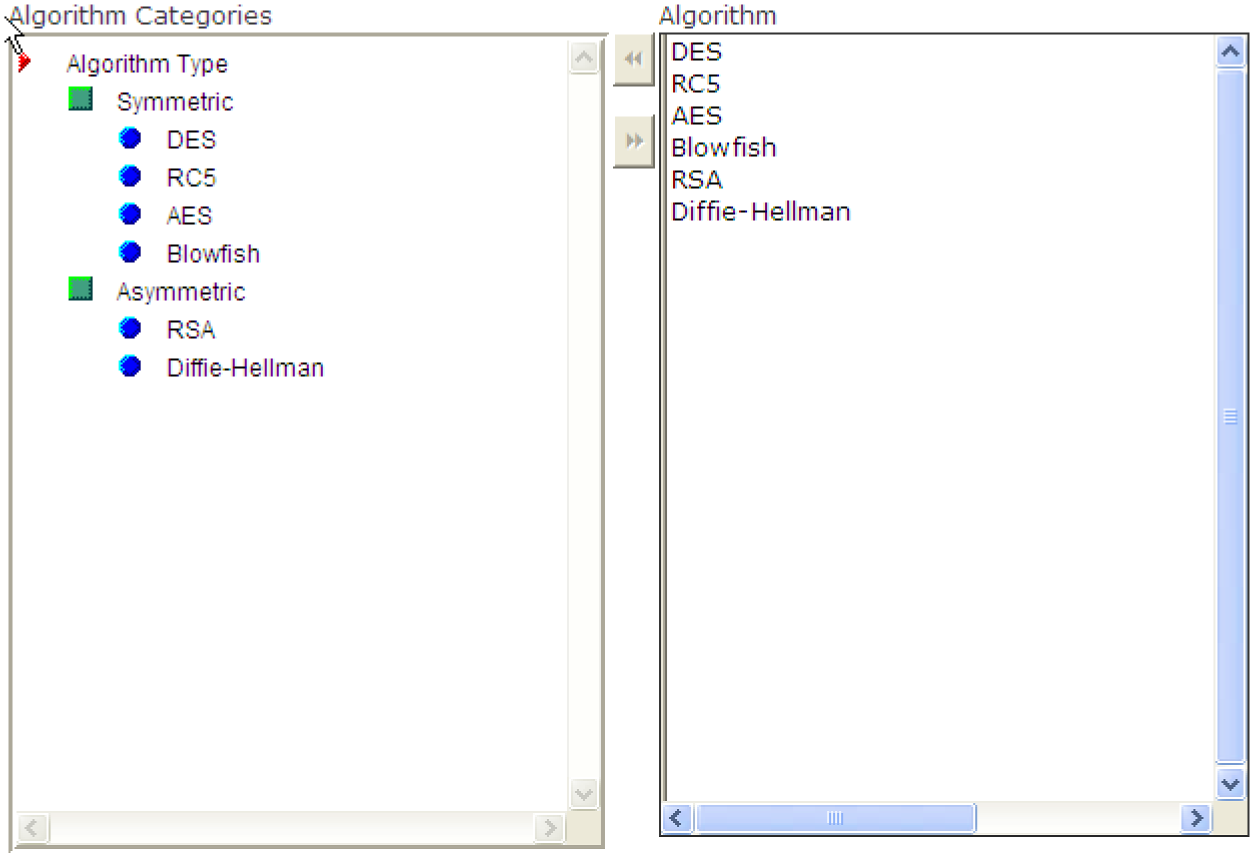
- Algorithm Type
  - 🟩 Symmetric
  - 🟩 Asymmetric

Algorithm

DES
RC5
AES
Blowfish
RSA
Diffie-Hellman

Options:

A- Algrithm Categories



Algorithm Categories

- Algorithm Type
  - Symmetric
    - DES
    - RC5
    - AES
    - Blowfish
  - Asymmetric
    - RSA
    - Diffie-Hellman

Algorithm

DES
RC5
AES
Blowfish
RSA
Diffie-Hellman

Answer:

A

Explanation:

DES

RC5

AES

Blowfish

Question 8

Question Type: MultipleChoice

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.

Options:

A- Executive summary

Answer:

A

Explanation:

efforts. It is useful for the security managers and DRP leaders as well as public relations personnel who require a non-technical perspective on

the disaster recovery effort.

Question 9

Question Type: MultipleChoice

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?

Options:

A- Single Sign-On

B- One-time password

C- Dynamic

D- Kerberos

Answer:

A

Explanation:

password to each application. In SSO, a user can access all computer applications and systems where he has access permission without

entering multiple passwords. This reduces human error and systems failure and is therefore highly desirable. There are many commercial SSO

solutions available in the market. Some of them are as follows:

Central Authentication Service (CAS)

The Dutch NREN

CoSign

Enterprise Single Sign-On (E-SSO)

Web Single Sign-On (Web SSO)

Security Assertion Markup Language (SAML)

Direct SSO

Shibboleth

Answer option B is incorrect. A one-time password (OTP) is a password only valid for a single login session or transaction. OTP avoids a

number of shortcomings that are associated with traditional passwords. The most important shortcoming that is addressed by OTP is that OTP

is not vulnerable to replay attacks. If a potential intruder manages to record an OTP that was already used to log into a service or to conduct

a transaction, he will not be able to abuse it since it will be no longer valid.

Answer option D is incorrect. Kerberos is a secure protocol that supports ticketing authentication. A ticket is granted in response to a client

computer authentication request by the Kerberos authentication server, if the request contains valid user credentials and a valid Service

Principal Name (SPN). The ticket is then used by the client computer to access network resources. To enable Kerberos authentication, the client and server computers must have a trusted connection to the domain Key Distribution Center (KDC). The task of KDC is to distribute

shared secret keys to enable encryption.

Answer option C is incorrect. In the dynamic password authentication scheme, passwords are changed after a specified time or time interval.

Question 10

Question Type: MultipleChoice

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?

Options:

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)

Answer:

D

Explanation:

necessary to make the communication as secure as possible. Also, the sales managers will be using laptops that are configured to read smart

cards. Therefore, they will use EAP, as it is highly secure and supports smart card authentication.

Question 11

Question Type: **MultipleChoice**

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

Options:

A- Fibre optic cable

B- STP cable

C- UTP cable

D- NTP cable

Answer:

A

Explanation:

traveling in fibre optic cables are not electrical signals. Therefore, they do not emit electromagnetic radiation and cannot be eavesdropped by

electromagnetic eavesdropping devices.

Answer options C and B are incorrect. In UTP and STP cables, the signals travel in electronic form and emit electromagnetic radiation.

Therefore, these cables are not secure against electronic eavesdropping.

Answer option D is incorrect. There is no cable such as NTP.