ISC2

ISSAP Exam

ISSAP Information Systems Security Architecture Professional

Questions & Answers
Demo

Question: 1

Which of the following elements of planning gap measures the gap between the total potential for the market and the actual current usage by all the consumers in the market?

A. Project gap
B. Product gap
C. Competitive gap
D. Usage gap

Answer: D

Explanation:
The usage gap measures the gap between the total potential for the market and the actual current usage by all the consumers in the market.
Mainly two figures are needed for this calculation:
Market potential: The maximum number of consumers available will usually be determined by market research, but it may sometimes be
calculated from demographic data or government statistics.
Existing usage: The existing usage by consumers makes up the total current market, from which market shares, for example, are
calculated. It is usually derived from marketing research, most accurately from panel research and also from ad hoc work.
Thus, the 'usage gap' can be calculated by:
usage gap = market potential - existing usage
Answer option B is incorrect. The product gap is also described as the segment or positioning gap. It represents that part of the market from
which the individual organization is excluded because of product or service characteristics. This may have come about because the market has
been segmented and the organization does not have offerings in some segments, or it may be because the positioning of its offering
effectively excludes it from certain groups of potential consumers, because there are competitive offerings much better placed in relation to
these groups.
The product gap is probably the main element of the planning gap in which the organization can have a productive input. Therefore the
emphasis is on the importance of correct positioning.
Answer option A is incorrect. The project gap is not a valid element of planning gap.
Answer option C is incorrect. The competitive gap is the share of business achieved among similar products, sold in the same market segment
and with similar distribution patterns or at least, in any comparison, after such effects have been discounted. The competitive gap represents
the effects of factors such as price and promotion, both the absolute level and the effectiveness of its messages. It is what marketing is
popularly supposed to be about.

Question: 2

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

Explanation:
Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet.
Answer option D is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer option C is incorrect. Web caching is a method for minimizing performance bottlenecks and reducing network traffic by serving locally cached Web content. Web caching helps in reducing bandwidth utilization during periods of high network traffic. High network traffic is usually caused when a large number of users use the network at the same time. With a caching solution in place, users' requests will be returned from the cache without having to travel over a WAN link to the destination Web server.
Answer option A is incorrect. Hacking is a process by which a person acquires illegal access to a computer or network through a security break or by implanting a virus on the computer or network.

Question: 3

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

A. PGP
B. PPTP
C. IPSec
D. NTFS

Answer: A

Explanation: Standard Internet e-mail is usually sent as plaintext over networks. This is not secure as intruders can monitor mail servers and network
traffic to obtain sensitive information. The two most commonly used methods for providing e-mail security are Pretty Good Privacy (PGP) and
Secure/Multipurpose Internet Mail Extensions (S/MIME). These methods typically include authentication of the originator and privacy of the
message.

Pretty Good Privacy (PGP) is an encryption method that uses public-key encryption to encrypt and digitally sign e-mail messages during
communication between e-mail clients. PGP is effective, easy to use, and free. Therefore, it is one of the most common ways to protect
messages on the Internet.

Answer option C is incorrect. Internet Protocol security (IPSec) provides secure communication over IP networks. It cannot be used to encrypt
e-mail messages.

Question: 4

Peter works as a Network Administrator for Net World Inc. The company wants to allow remote users to connect and access its private network through a dial-up connection via the Internet. All the data will be sent across a public network. For security reasons, the management wants the data sent through the Internet to be encrypted. The company plans to use a Layer 2 Tunneling Protocol (L2TP) connection. Which communication protocol will Peter use to accomplish the task?

A. IP Security (IPSec)
B. Microsoft Point-to-Point Encryption (MPPE)
C. Pretty Good Privacy (PGP)
D. Data Encryption Standard (DES)

Answer: A

Explanation: According to the question, all the data will be sent across a public network. Data sent through a public network such as the Internet should
be encrypted in order to maintain security.

The two modes available for data encryption are Microsoft Point-to-Point Encryption (MPPE) and IP Security (IPSec). The MPPE protocol is used
for data encryption in a PPTP connection. It supports MSCHAP v1 and v2, and the EAP-TLS authentication methods. However, L2TP does not
support the MPPE protocol. Therefore, for an L2TP connection, Peter will have to use the IPSec protocol to encrypt data. L2TP with IPSec
needs a certificate authority server (CA server) to generate certificates as well as to check their validity for providing secure communication
across both ends of the VPN.

Question: 5

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

Explanation: Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices
in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively
used for gaming and showing online videos. IGMP is vulnerable to network attacks.
Answer option B is incorrect. Internet Control Message Protocol (ICMP) is an integral part of IP. It is used to report an error in datagram
processing. The Internet Protocol (IP) is used for host-to-host datagram service in a network. The network is configured with connecting
devices called gateways. When an error occurs in datagram processing, gateways or destination hosts report the error to the source hosts
through the ICMP protocol. The ICMP messages are sent in various situations, such as when a datagram cannot reach its destination, when
the gateway cannot direct the host to send traffic on a shorter route, when the gateway does not have the buffering capacity, etc.
Answer option A is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is
responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is
used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this
correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.
Answer option C is incorrect. Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol operating at the transport layer of
the OSI model. It provides a reliable packet delivery service encapsulated within the Internet Protocol (IP). TCP guarantees the delivery of
packets, ensures proper sequencing of data, and provides a checksum feature that validates both the packet header and its data for
accuracy. If the network corrupts or loses a TCP packet during transmission, TCP is responsible for retransmitting the faulty packet. It can
transmit large amounts of data. Application-layer protocols, such as HTTP and FTP, utilize the services of TCP to transfer files between clients
and servers.

Question: 6

Which of the following security devices is presented to indicate some feat of service, a special

accomplishment, a symbol of authority granted by taking an oath, a sign of legitimate employment or student status, or as a simple means of identification?

A. Sensor
B. Alarm
C. Motion detector
D. Badge

Answer: D

Explanation: A badge is a device or accoutrement that is presented or displayed to indicate some feat of service, a special accomplishment, a symbol of
authority granted by taking an oath, a sign of legitimate employment or student status, or as a simple means of identification. It is also used
in advertising, publicity, and for branding purposes.
A badge can be made from metal, plastic, leather, textile, rubber, etc., and it is commonly attached to clothing, bags, footwear, vehicles, home
electrical equipment, etc.
Answer option A is incorrect. A sensor is a device that measures a physical quantity and converts it into a signal that can be read by an
observer or by an instrument.
Answer option C is incorrect. A motion detector 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.
They form a vital component of comprehensive security systems, for both homes and businesses.
Answer option B is incorrect. An alarm is a device that triggers a deterrent, a repellent, and a notification.

Question: 7

Which of the following is a method for transforming a message into a masked form, together with a way of undoing the transformation to recover the message?

A. Cipher
B. CrypTool
C. Steganography
D. MIME

Answer: A

Explanation: A cipher is a cryptographic algorithm that performs encryption or decryption. It is a series of well-defined steps that can be followed as a
procedure. The cipher transforms a message into a masked form, together with a way of undoing the transformation to recover the message.
When using a cipher the original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all
the information of the plaintext message, but it is not in a readable format.

The operation of a cipher usually depends on a piece of auxiliary information, called a key or a cryptovariable. The encrypting procedure is
varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt
a message. Without knowledge of the key, it is impossible to decrypt the ciphertext into plaintext.
Answer option B is incorrect. CrypTool is free software and an e-learning tool illustrating cryptographic concepts.
Answer option C is incorrect. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the
sender and intended recipient, suspects the existence of the message, a form of security through obscurity.
Answer option D is incorrect. MIME stands for Multipurpose Internet Mail Extensions. It is a standard for multi-part, multimedia electronic mail
messages and World Wide Web hypertext documents on the Internet. MIME provides a mechanism for exchanging non-text information, such
as binary data, audio data, video data, and foreign language text that cannot be represented in ASCII text.

Question: 8

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

A. Policy Access Control
B. Mandatory Access Control
C. Discretionary Access Control
D. Role-Based Access Control

Answer: D

Explanation: Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the
organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to
access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also
be handled using the RBAC model.
Answer option B is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the
system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an
object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant
permission to other users to see this object unless they have the appropriate permission.
Answer option C is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data.
This model is commonly used in PC environment. The basis of this model is the use of Access Control List (ACL).

Answer option A is incorrect. There is no such access control model as Policy Access Control.

Question: 9

Which of the following is used to authenticate asymmetric keys?

A. Digital signature
B. MAC Address
C. Demilitarized zone (DMZ)
D. Password

Answer: A

Explanation: A digital signature is used to authenticate asymmetric keys.
Digital signature is a message signed with a sender's private key can be verified by anyone who has access to the sender's public key,
thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity.
Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which the key used to encrypt a message
differs from the key used to decrypt it.
Answer option C is incorrect. Demilitarized zone (DMZ) or perimeter network is a small network that lies in between the Internet and a private
network. It is the boundary between the Internet and an internal network, usually a combination of firewalls and bastion hosts that are
gateways between inside networks and outside networks. DMZ provides a large enterprise network or corporate network the ability to use
the Internet while still maintaining its security.
Answer options D and B are incorrect. Password and MAC address are not used to authenticate asymmetric keys.

Question: 10

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: D and C

Explanation: IPsec VPN provides a high degree of data privacy by establishing trust points between communicating devices and data encryption using the
3DES (Triple Data Encryption Algorithm) or AES (Advanced Encryption Standard).