SY0-401Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-401 Exam with 100% Guarantee

QUESTION 1

A risk management team indicated an elevated level of risk due to the location of a corporate datacenter in a region with an unstable political climate. The chief information officer (CIO) accepts the recommendation to transition the workload to an alternate datacenter in a more stable region. Which of the following forms of risk mitigation has the CIO elected to pursue?

A. Deterrence

B. Transference

C. Avoidance

D. Acceptance

E. sharing

Correct Answer: C

QUESTION 2

Which of the following firewall rules only denies DNS zone transfers?

A. deny udp any any port 53

B. deny ip any any

C. deny tcp any any port 53

D. deny all dns packets

Correct Answer: C

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers.

QUESTION 3

Joe has been in the same IT position for the last 27 years and has developed a lot of the homegrown applications that the company utilizes. The company is concerned that Joe is the only who can administer these applications. The company should enforce which of the following best security practices to avoid Joe being a single point of failure?

A. Separation of Duties

B. Least privilege

C. Job rotation

D. Mandatory vacations

Correct Answer: C

QUESTION 4

A computer is put into a restricted VLAN until the computer\\'s virus definitions are up-to- date.

Which of the following BEST describes this system type?

A. NAT

B. NIPS

C. NAC

D. DMZ

Correct Answer: C

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

QUESTION 5

A security technician received notification of a remotely exploitable vulnerability affecting all multifunction printers firmware installed throughout the organization. The vulnerability allows a malicious user to review all the documents processed by the affected printers. Which of the following compensating controls can the security technician to mitigate the security risk of a sensitive document leak?

A. Create a separate printer network

B. Perform penetration testing to rule out false positives

C. Install patches on the print server

D. Run a full vulnerability scan of all the printers

Correct Answer: C

QUESTION 6

A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?

A. SMTP

B. iSCSI

C. SNMP

D. IPSec

Correct Answer: C

QUESTION 7

A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

A. It provides authentication services

B. It uses tickets to identify authenticated users

C. It provides single sign-on capability

D. It uses XML for cross-platform interoperability

Correct Answer: B

QUESTION 8

Which of the following ciphers would be BEST used to encrypt streaming video?

A. RSA

B. RC4

C. SHA1

D. 3DES

Correct Answer: B

In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP.

Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit-flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly. Furthermore, inadvertent double encryption of a message with the same key may accidentally output plaintext rather than ciphertext because the involutory nature of the XOR function would result in the second operation reversing the first. It is noteworthy, however, that RC4, being a stream cipher, was for a period of time the only common cipher that was immune to the 2011 BEAST attack on TLS 1.0. The attack exploits a known weakness in the way cipher block chaining mode is used with all of the other ciphers supported by TLS 1.0, which are all block ciphers.

QUESTION 9

Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP

B. SNMP

C. SFTP

D. SCP

E. TFTP

Correct Answer: CD

Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks. SFTP is a secured alternative to standard FTP. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

QUESTION 10

The helpdesk is receiving numerous reports that a newly installed biometric reader at the entrance of the data center has a high of false negatives. Which of the following is the consequence of this reported problem?

A. Unauthorized employees have access to sensitive systems

B. All employees will have access to sensitive systems

C. No employees will be able to access the datacenter

D. Authorized employees cannot access sensitive systems

Correct Answer: C

QUESTION 11

Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

A. Trust model

B. Public Key Infrastructure

C. Private key

D. Key escrow

Correct Answer: D

Sensitive PKI data, such as private keys, can be put into key escrow data. The key escrow data can be kept at a trusted third party.

Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses,

who may want access to employees\\' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

QUESTION 12

A network administrator has identified port 21 being open and the lack of an IDS as a potential risk to the company. Due to budget constraints, FTP is the only option that the company can is to transfer data and network equipment cannot be purchased. Which of the following is this known as?

A. Risk transference

B. Risk deterrence

C. Risk acceptance

D. Risk avoidance

Correct Answer: C

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

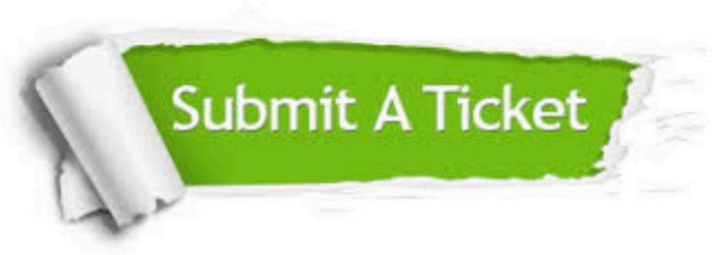
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.