98-367$^{\text{Q\&As}}$

Security Fundamentals

Pass Microsoft 98-367 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/98-367.html

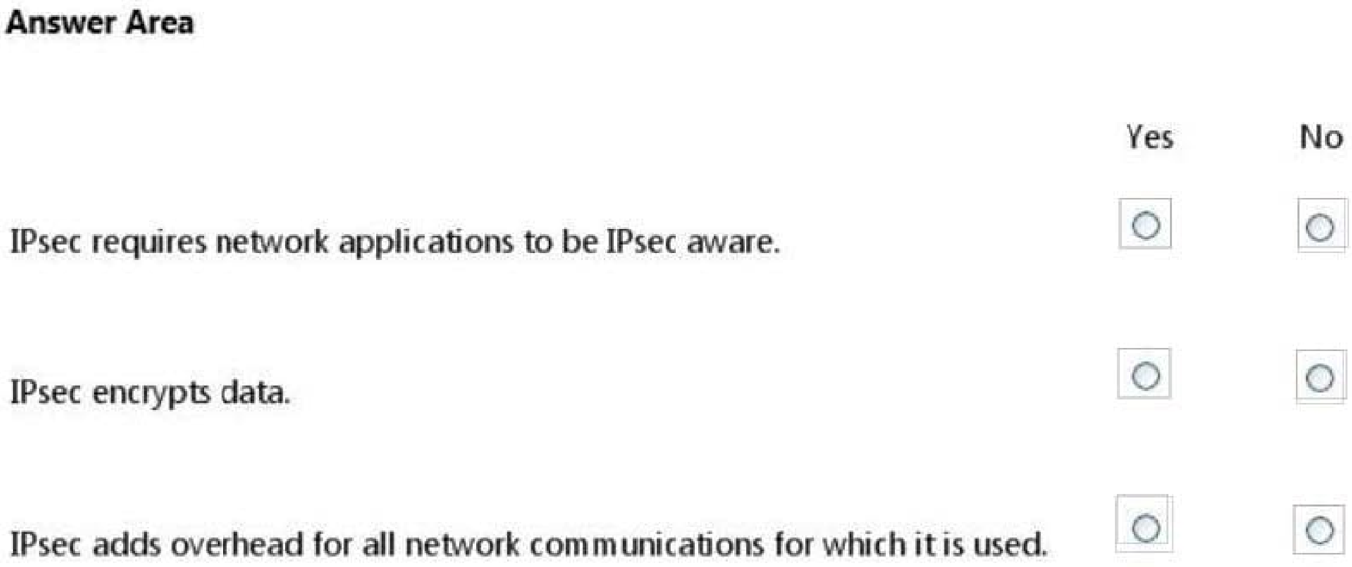
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

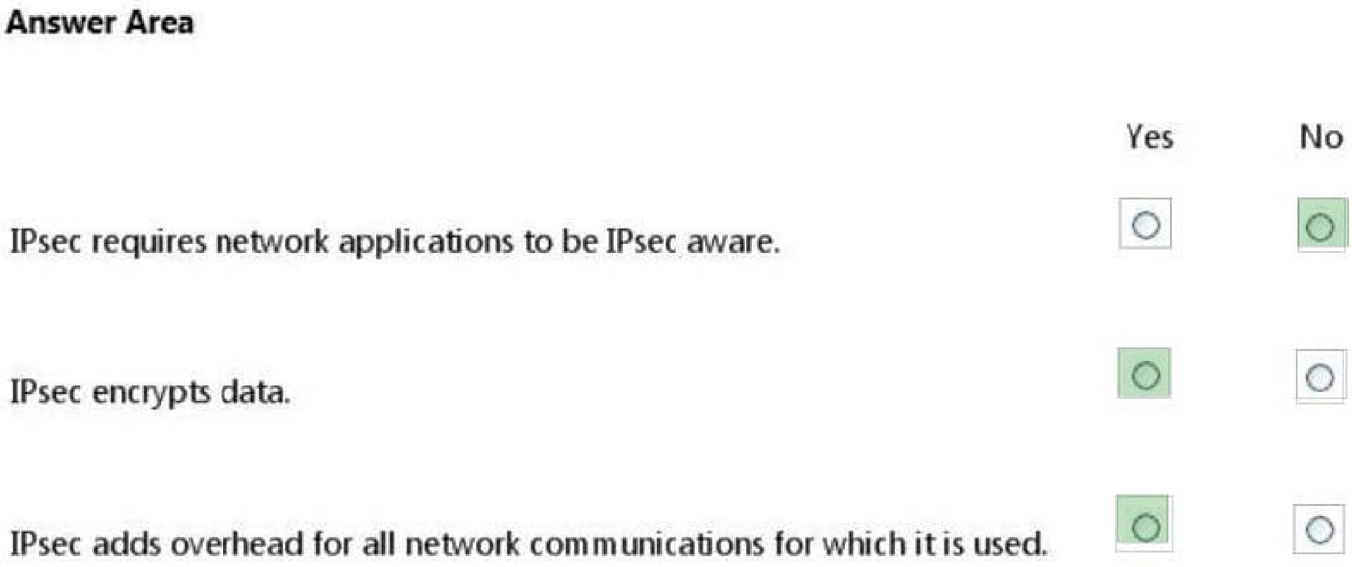
Hot Area:



Answer Area

	Yes	No
IPsec requires network applications to be IPsec aware.	○	○
IPsec encrypts data.	○	○
IPsec adds overhead for all network communications for which it is used.	○	○

Correct Answer:



Answer Area

	Yes	No
IPsec requires network applications to be IPsec aware.	○	●
IPsec encrypts data.	●	○
IPsec adds overhead for all network communications for which it is used.	●	○

QUESTION 2

A process by which DNS zone data is obtained by an attacker is referred to as:

A. spoofing

B. footprinting

C. phishing

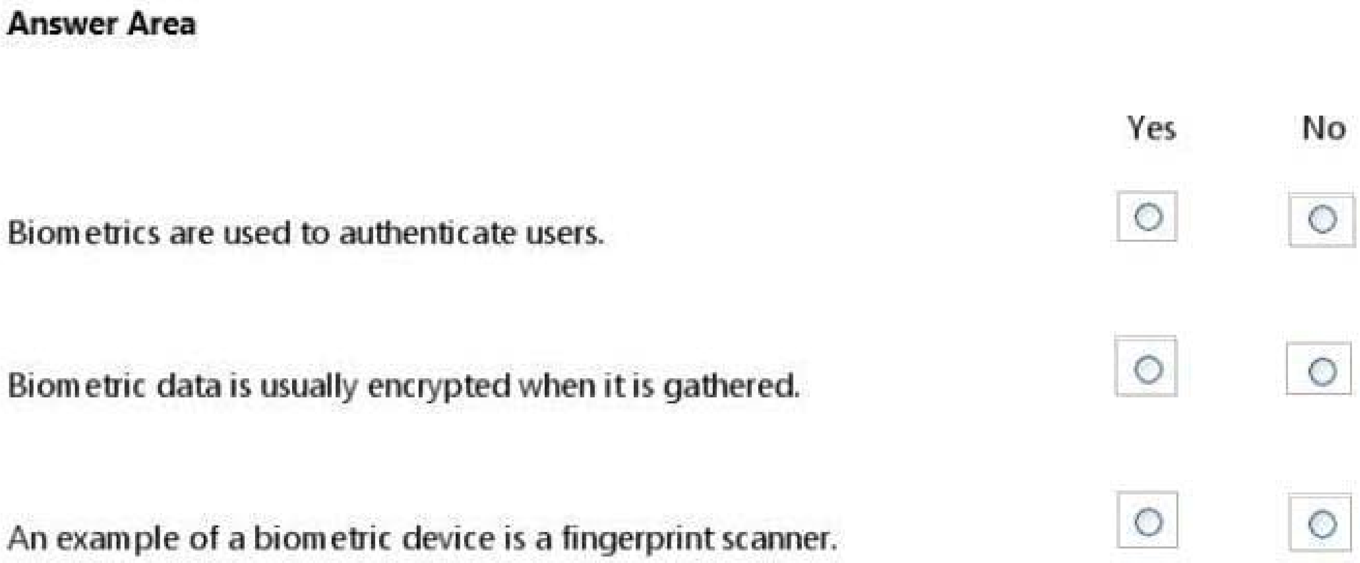
D. Denial of Service

Correct Answer: B

QUESTION 3

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

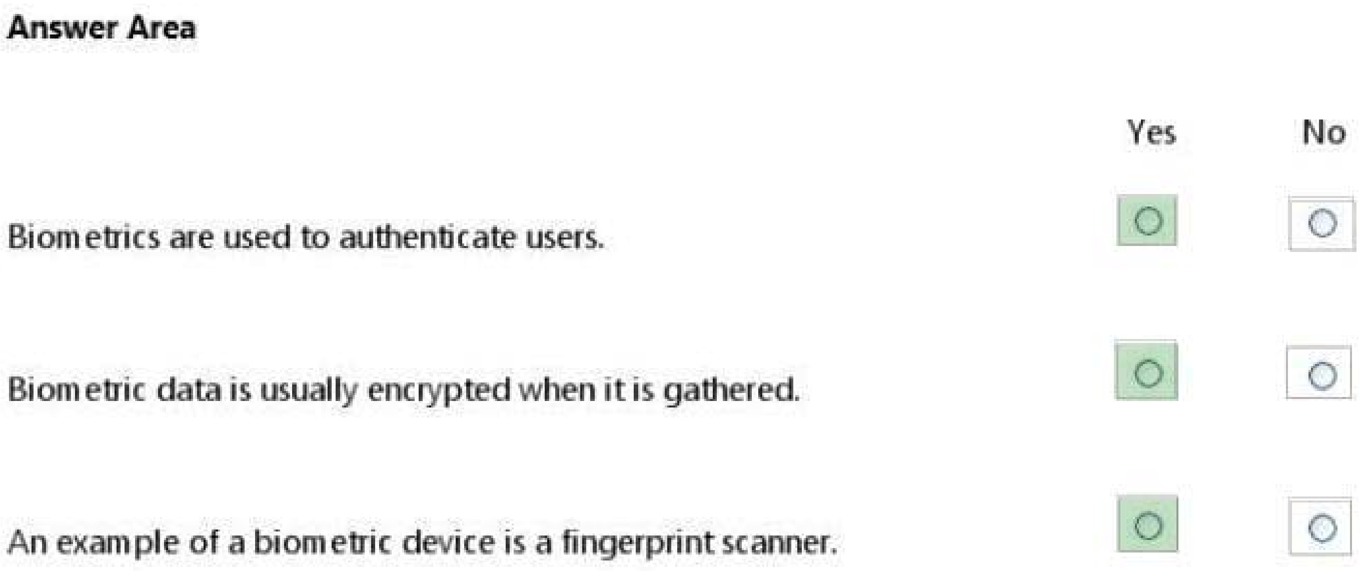
Hot Area:



Answer Area

	Yes	No
Biometrics are used to authenticate users.	○	○
Biometric data is usually encrypted when it is gathered.	○	○
An example of a biometric device is a fingerprint scanner.	○	○

Correct Answer:



Answer Area

	Yes	No
Biometrics are used to authenticate users.	[✓ ○]	○
Biometric data is usually encrypted when it is gathered.	[✓ ○]	○
An example of a biometric device is a fingerprint scanner.	[✓ ○]	○

Biometric devices, such as finger scanners consist of a reader or scanning device, Software that converts the scanned information into digital form and compares match points, and a database that stores the biometric data for comparison. To prevent identity theft, biometric data is usually encrypted when it is gathered.

QUESTION 4

A user who receives a large number of emails selling prescription medicine is probably receiving pharming mail.

Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed" if the underlined text makes the statement correct.

A. Malware

B. Spoofed mail

C. Spam

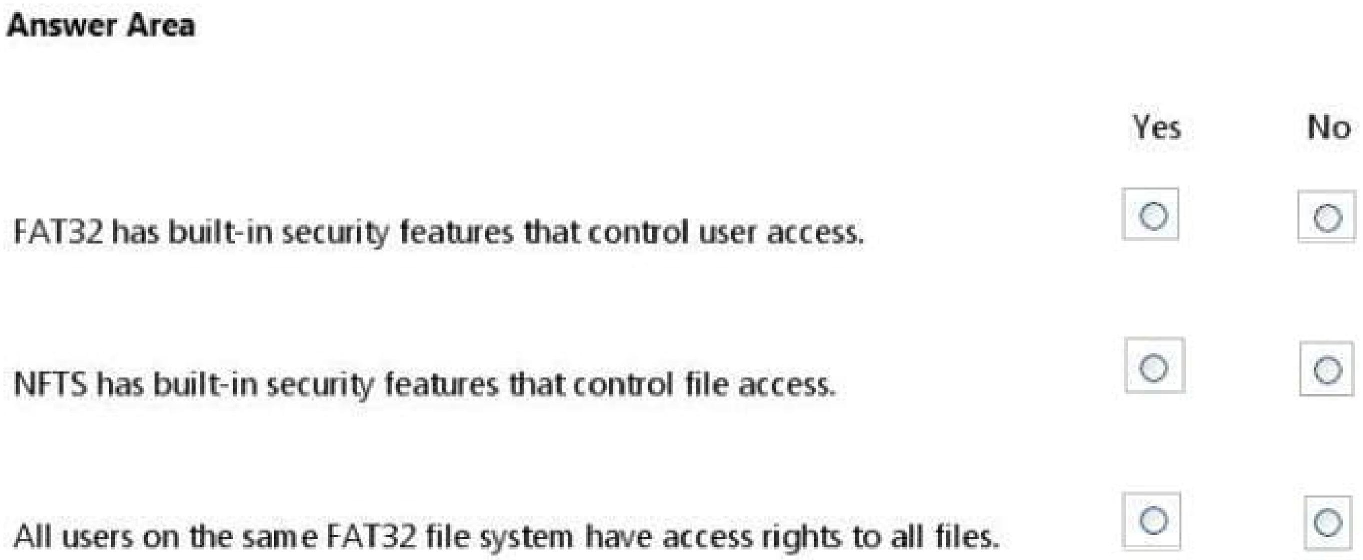
D. No change is needed.

Correct Answer: C

QUESTION 5

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

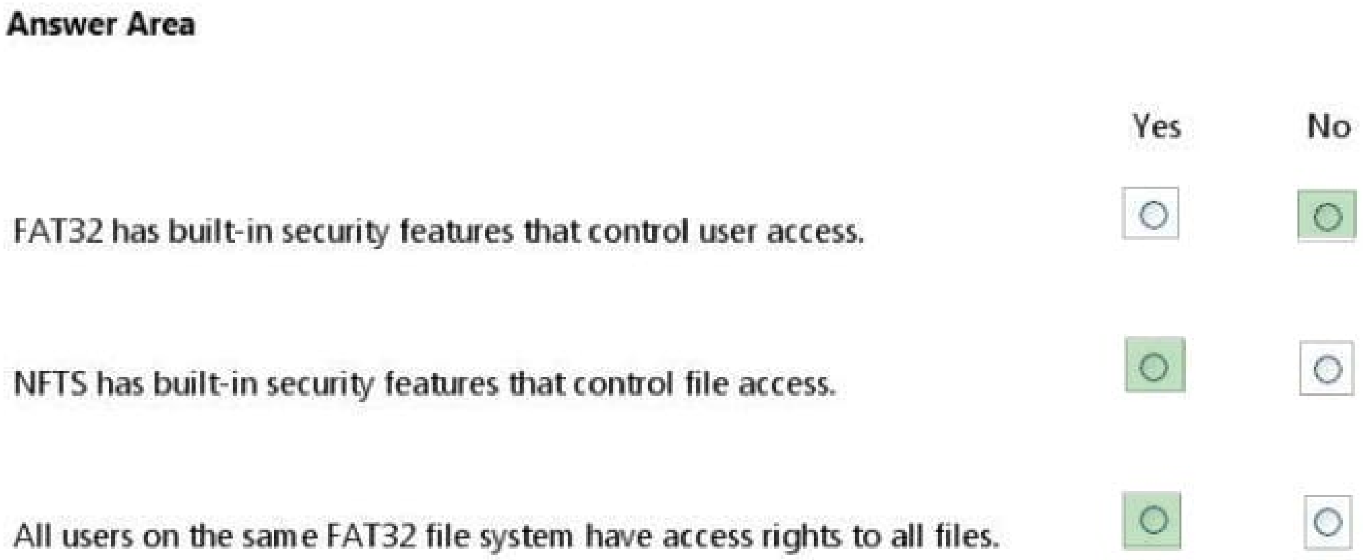
Hot Area:



Answer Area

	Yes	No
FAT32 has built-in security features that control user access.	○	○
NFTS has built-in security features that control file access.	○	○
All users on the same FAT32 file system have access rights to all files.	○	○

Correct Answer:



Answer Area

	Yes	No
FAT32 has built-in security features that control user access.	○	[✓ ○]
NFTS has built-in security features that control file access.	[✓ ○]	○
All users on the same FAT32 file system have access rights to all files.	[✓ ○]	○

QUESTION 6

Which of the following is a secret numeric password shared between a user and a system for authenticating the user to the system?

A. PIN

B. Private key

C. Key escrow

D. Public key

Correct Answer: A

A personal identification number (PIN) is a secret numeric password shared between a user and a system for authenticating the user to the system. Answer: C is incorrect. 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. Answer: B is incorrect. In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. Answer: D is incorrect. A Public Key is known commonly to everybody. It is used to encrypt data. Only specific users can decrypt it. Data encryption is used to encrypt data so that it can only be decrypted with the corresponding private key owned by the public key owner. The public key is also used to verify digital signatures. This signature is created by the associated private key.

QUESTION 7

What is a service set identifier (SSID)?

A. A wireless encryption standard

B. The wireless LAN transmission type

C. The broadcast name of an access point

D. A wireless security protocol

Correct Answer: C

SSID (service set identifier) is a function performed by an Access Point that transmits its name so that wireless stations searching for a network connection can \\'discover\\' it. It\\'s what allows your wireless adapter\\'s client manager program or Windows built-in wireless software to give you a list of the Access Points in range.

QUESTION 8

You need to prevent unauthorized users from reading a specific file on a portable computer if the portable computer is stolen.

What should you implement?

A. File-level permissions

B. Advanced Encryption Standard (AES)

C. Folder-level permissions

D. Distributed File System (DFS)

E. BitLocker

Correct Answer: E

Reference: http://4sysops.com/archives/seven-reasons-why-you-need-bitlocker-hard-drive-encryption-for-your-whole-organization/

QUESTION 9

You manage 50 Windows workstations in a computer lab. All workstations belong to the lab Active Directory domain.

You need to implement several audit policies on each workstation in the shortest time possible.

What should you do?

A. Enable logging on each computer

B. Create a domain Group Policy

C. Turn on the Audit Policy on the domain controller

D. Enable Audit object access

Correct Answer: B

References:

https://docs.microsoft.com/en-us/windows-server/networking/branchcache/deploy/use-group-policy-to- configure-domain-member-client-computers

QUESTION 10

To keep third-party content providers from tracking your movements on the web, enable InPrivate Browsing.

Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed\\'\\' if the underlined text makes the statement correct.

A. InPrivate Filtering

B. SmartScreen Filter

C. Compatibility Mode

D. No change is needed

Correct Answer: A

QUESTION 11

Mark works as a Network Administrator fot Blue Well Inc. The company has a Windows-based network. Mark is facing a series of problems with email spam and identifying theft via phishing scams. He wants to implement the various security measures and to provide some education because it is related to the best practices while using email. Which of the following can Mark use to minimize the spam amount that is hitting the Microsoft Exchange server of the company?

A. Enable reverse DNS lookup

B. Use Read-only Domain Controller

C. Add Sender Policy Framework

D. Permit User Account Control

Correct Answer: A

To minimize the amount of spam that is hitting the Microsoft Exchange server, it is required to enable reverse DNS lookup on the SMTP virtual server. It forces a system to crosscheck the domain name with a PTR record (IP address

associated with the domain name) and if the IP address is not matched the record associated with that domain name, it will not delivered.

Answer: C is incorrect. SPF is used to permit the administrator to configure the server to establish who is acceptable to send email from their domain. Answer: D is incorrect. User Account Control (UAC) is a technology and security

infrastructure introduced with Microsoft\\'s Windows Vista and Windows Server 2008 operating systems, with a more relaxed version also present in Windows 7 and Windows Server 2008 R2. It aims to improve the security of Microsoft

Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation.

Answer: B is incorrect. Read-only Domain Controller (RODC) is a domain controller that hosts the read-only partition of the Active Directory database. RODC was developed by Microsoft typically to be deployed in a branch office environment.

RODC is a good option to enhance security by placing it in a location where physical security is poor. RODC can also be placed at locations having relatively few users and a poor network bandwidth to the main site. As only the read-only

partition of the Active Directory database is hosted by RODC, a little local IT knowledge is required to maintain it.

QUESTION 12

A brute force attack:

A. Uses response filtering

B. Tries all possible password variations

C. Uses the strongest possible algorithms

D. Targets all the ports

Correct Answer: B

QUESTION 13

This question requires that you evaluate the underlined text to determine if it is correct.

Dedicated perimeter firewalls often provide a service named static packet filtering, which converts interval private addresses into an external Internet address.

Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed." If the statement is incorrect, select the answer choice that makes the statement correct.

A. Application Layer filtering

B. Network Address Translation

C. circuit-level inspection

D. No change is needed

Correct Answer: B

References:

http://www.excitingip.com/205/what-are-packet-filtering-circuit-level-application-level-and-stateful- multilayer-inspection-firewalls/

QUESTION 14

E-mail spoofing:

A. Forwards e-mail messages to all contacts

B. Copies e-mail messages sent from a specific user

C. Obscures the true e-mail sender

D. Modifies e-mail routing logs

Correct Answer: C

Reference: http://www.microsoft.com/mscorp/safety/technologies/senderid/technology.mspx

QUESTION 15

You check the logs on several clients and find that there is traffic coming in on an odd port (port 1872). All clients have the Windows XP firewall turned on. What should you do to block this unwanted traffic?

A. Perform a virus scan to find the virus responsible for this traffic.

B. Check the exceptions in the firewall and unselect that port exception.

C. Trace back that traffic and find its origin.

D. Shut down the service that connects to that port.

Correct Answer: B

The Windows firewall has an exception list of applications and ports that are allowed to pass through the firewall. Find this port and remove it from the exception list.