98-367 Q&As

Security Fundamentals

Pass Microsoft 98-367 Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Coho Winery wants to increase their web presence and hires you to set up a new web server. Coho already has servers for their business and would like to avoid purchasing a new one. Which server is best to use as a web server, considering the security and performance concerns?

A. SQL Server

B. File Server

C. Domain Controller

D. Application Server

Correct Answer: C

QUESTION 2

Mark works as a Security Officer for TechMart Inc. The company has a Windows- based network. He has bees assigned a project for ensuring the safety of the customer\\'s money and information, not to mention the company\\'s reputation. The company has gone through a security audit to ensure that it is in compliance with industry regulations and standards. Mark understands the request and has to do his due diligence for providing any information the regulators require as they are targeting potential security holes. In this situation, his major concern is the physical security of his company\\'s system. He has a concern that people are authenticated to the servers in the data center. Which of the following actions will Mark take to prevent normal users from logging onto the systems?

A. Call a team member while behaving to be someone else for gaining access to sensitive information.

B. Use group policies to disable the use of floppy drives or USB drives.

C. Provide protection against a Distributed Denial of Services attack.

D. Develop a social awareness of security threats within an organization.

Correct Answer: B

To prevent normal users from logging onto the systems, it is required to create a group policy that can be applied to the servers to Deny Log on Locally for all non- administrative users. It will create a problem for the people who are in the data

center with physical access. However, normal users should not have the ability to log on locally.

Answer: C While stressing the Con?dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

QUESTION 3

Which of the following types of attack is used to configure a computer to behave as another computer on a trusted network by using the IP address or the physical address?

A. Distributed denial of service (DDOS) attack

B. Honeypot

C. RIP/SAP Spoofing

D. Identity spoofing

Correct Answer: D

Identity spoofing (IP address spoofing) will occur when the attacker wants to use an IP address of a network, computer, or network component without being authorized for this task. It allows the unprivileged code to use someone else\\'s identity, and use their security credentials Answer: B is incorrect. A honey pot is a computer that is used to attract potential intruders or attackers. It is for this reason that a honey pot has low security permissions. A honey pot is used to gain information about the intruders and their attack strategies. Answer: C is incorrect. RIP and SAP are used to broadcast network information in a regular way regardless of no changes in the routing or service tables. RIP/SAP spoofing method is used to intercept the SAP and RIP broadcasts by using a spoofing modem/router, and then re-broadcast network information via its own routing table or service table. Answer: A is incorrect. In the distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that it has previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for the DDoS attack.

QUESTION 4

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
Tools like Microsoft Security Compliance Manager and Microsoft Baseline Security Analyzer can assist with server hardening.	○	○
Administrator passwords may contain ASCII characters generated by a combination of the ALT key and three digits on the numeric keypad.	○	○
The removal of unused registry entries and executables increases the surface vulnerability of the server.	○	○

Correct Answer:

Answer Area

	Yes	No
Tools like Microsoft Security Compliance Manager and Microsoft Baseline Security Analyzer can assist with server hardening.	○	○
Administrator passwords may contain ASCII characters generated by a combination of the ALT key and three digits on the numeric keypad.	○	○
The removal of unused registry entries and executables increases the surface vulnerability of the server.	○	○

QUESTION 5

Before you deploy Network Access Protection (NAP), you must install:

A. Internet Information Server (IIS)

B. Network Policy Server (NPS)

C. Active Directory Federation Services

D. Windows Update Service

Correct Answer: B

Reference: http://technet.microsoft.com/en-us/library/bb681008.aspx

QUESTION 6

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 7

Mark works as a Network Administrator for TechMart Inc. The company has a Windows-based network. Mark wants to implement a method to ensure that the mobile devices are in a good state of security health when they are trying to access the corporate network. Which of the following is a control or strategy that Mark will implement to assure the security health?

A. TCP/IP protocol

B. Kerberos

C. Single Sign On

D. Network Access Protection

Correct Answer: D

Network Access Protection (NAP) is a set of operating system components included with the Windows Server 2008 and Windows Vista/7 operating systems. It ensures that the client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer\\'s operating system and critical software. For example, an administrator can set policies that computers might be required to have antivirus software with the latest virus definition installed and current operating system updates. Using NAP, a network administrator can enforce compliance with health requirements for the client computers connection to the network. NAP helps network administrators to reduce the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software. Answer: C is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times. Answer: B is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: A is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

QUESTION 8

The purpose of Windows Server Update Services (WSUS) is to:

A. manage the deployment of patches to company servers

B. provide alerts and reports on system vulnerabilities

C. set permissions to the minimum level necessary for each function

D. update licensing for Windows servers

Correct Answer: A

QUESTION 9

In which of the following is the file audit events are written when auditing is enabled?

A. File system ACL

B. Biometric device

C. Network Access Control List

D. Security event log

Correct Answer: D

The various enabled file auditing events are documented and written in the security event log Answer: A is incorrect. A filesystem ACL is deifned as a data structure (usually a table) that contains entries specifying individual user or group rights to specific system objects like programs, processes, or files. These entries are known as access control entries (ACEs) in the Microsoft Windows NT, OpenVMS, Unix-like, and Mac OS X operating systems and each of the accessible object contains an identifier to its ACL. The permissions are used to find the particular access rights, such as

whether a user is able to read from, write to, or execute an object. Answer: C is incorrect. Network Access Control List is defined as a set of rules applied to port numbers or network daemon names that are available on a host or other layer 3, and attached with a list of hosts and networks permitted to use the various defined service. The individual servers and routers can have network ACLs. It is used to control both inbound and outbound traffic as firewall does. Answer: B is incorrect. A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits. Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided into two main classes: 1.Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent. 2.Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

QUESTION 10

What is the standard or basic collection of NTFS permissions?

A. Read and execute, read, write, full control, modify, list folder contents

B. Change permissions, read permissions, write permissions

C. Read attributes, list folder/read data, traverse folder/execute file

D. Create files/write data, create folders/append data, take ownership

Correct Answer: A

Reference: http://technet.microsoft.com/en-us/library/bb727008.aspx

QUESTION 11

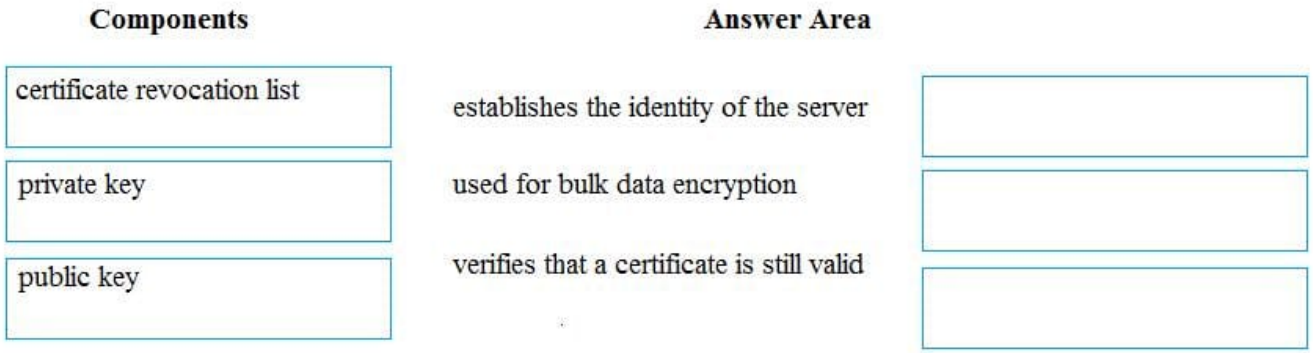
Match the components of a secure website with their role in securing communication.

Instructions: To answer, drag the appropriate component from the column on the left to its role on the right.

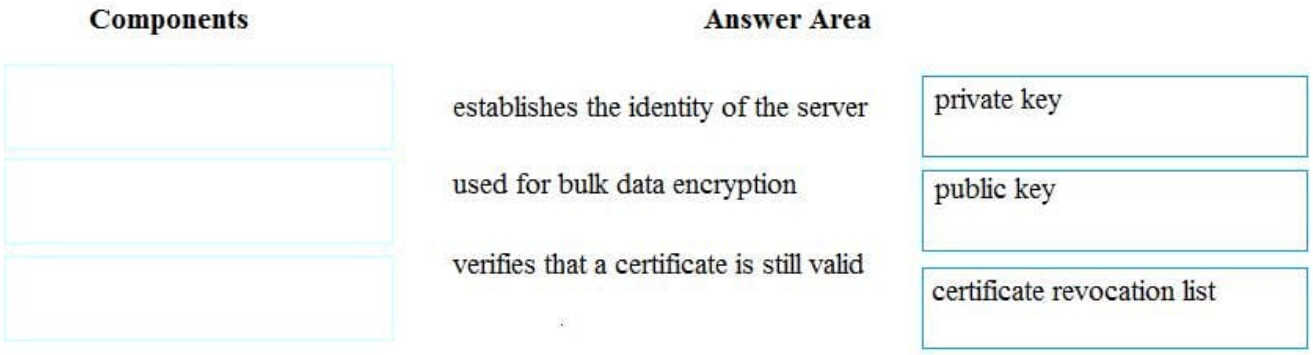
Each component may be used once, more than once or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



QUESTION 12

What are three examples of two-factor authentication? (Choose three.)

A. A fingerprint and a pattern

B. A password and a smart card

C. A username and a password

D. A password and a pin number

E. A pin number and a debit card

Correct Answer: ABE

At minimum two-factor authentication requires two out of three regulatory-approved authentication variables such as:

Something you know (like the PIN on your bank card or email password).

Something you have (the physical bank card or a authenticator token).

Something you are (biometrics like your finger print or iris pattern).

QUESTION 13

In Internet Explorer 8, the InPrivate Browsing feature prevents:

A. Unauthorized private data input.

B. Unencrypted communication between the client computer and the server.

C. User credentials from being sent over the Internet.

D. Any session data from being stored on the computer.

Correct Answer: D

Reference: http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing

QUESTION 14

To prevent users from copying data to removable media, you should:

A. Lock the computer cases

B. Apply a group policy

C. Disable copy and paste

D. Store media in a locked room

Correct Answer: B

Reference: http://blogs.technet.com/b/askds/archive/2008/08/25/removable-storage-group-policy-and-windows-server-2008-and-windows-vista.aspx

QUESTION 15

You work as a Network Administrator for NetTech Inc. You want to prevent users from accessing the graphical user interface (GUI) on the computers in the network. What will you do to accomplish this task?

A. Implement a remote access policy

B. Implement a group policy

C. Apply NTFS permission

D. Implement an account policy

Correct Answer: B

In order to prevent users from accessing the graphical user interface (GUI) on the computers in the network, you will have to implement a group policy. A group policy that is created by an administrator affects all users on a computer or all users on a domain. Group policies can be used for defining, customizing, and controlling the functioning of network

resources, computers, and operating systems. They can be set for a single computer with multiple users, for users in workgroups, or for computers in a domain. Administrators can configure group policy settings for users as well as for computers in many ways. Group policies can be used to allow or restrict the access of a particular program by a particular user. It can also be used to configure the desktop, the Start menu, the taskbar, the Control Panel, security settings, among other things. In Windows XP, group policies can be configured by using the Group Policy Console dialog box, which can be opened by running the GPEDIT.MSC command from the Start menu. Answer: D is incorrect. An account policy controls the password expiration policy, the lockout policy, and other password features. Answer: A is incorrect. A remote access policy specifies how remote users can connect to the network and the requirements for each of their systems before they are allowed to connect. It defines the methods users can use to connect remotely such as dial up or VPN. This policy is used to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data. Answer: C is incorrect. Applying NTFS permission will not help in accomplishing the task.