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.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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

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
DNSSEC prevents spoofing of query responses.	○	○
Clients can verify that the DNS server that they are communicating with is legitimate.	○	○
DNSSEC prevents man-in-the-middle attacks for DNS queries.	○	○

Correct Answer:

Answer Area

	Yes	No
DNSSEC prevents spoofing of query responses.	●	○
Clients can verify that the DNS server that they are communicating with is legitimate.	●	○
DNSSEC prevents man-in-the-middle attacks for DNS queries.	●	○

QUESTION 2

The process of creating a barrier between domain members and non-domain members by using IPsec policies is referred to as:

A. server filtering

B. domain filtering

C. domain isolation

D. server isolation

Correct Answer: C

References: https://blogs.msdn.microsoft.com/james_morey/2005/04/21/what-the-heck-is-domain-isolation/

QUESTION 3

Which of the following are types of password policies of Windows 7? Each correct answer represents a complete solution. Choose all that apply.

A. Store Password Using Reversible Encryption

B. Minimum Password Length

C. User Name Length

D. Password Must Meet Complexity Requirements

Correct Answer: ABD

Answer: B, A, and D Password policies are account policies that are related to user accounts. These policies increase the effectiveness of users\\' passwords by enforcing different types of controls on their usage. In Windows 7, there are following six types of password policies that can be configured by administrators: Enforce Password History Maximum Password Age Minimum Password Age Minimum Password Length Password Must Meet Complexity Requirements Store Password Using Reversible Encryption These options are disabled by default. However, an administrator can enable any option in the Local Security Settings tool, which can be accessed from the Administrative tools window found under Control Panel. Answer: C is incorrect. User name length does not come under password policies.

QUESTION 4

The reason for implementing Service Set IDentifier (SSID) masking is to:

A. enforce a more secure password policy

B. hide a wireless network name from unknown computers

C. hide a network share from unauthorized users

D. disable autologon

Correct Answer: B

QUESTION 5

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