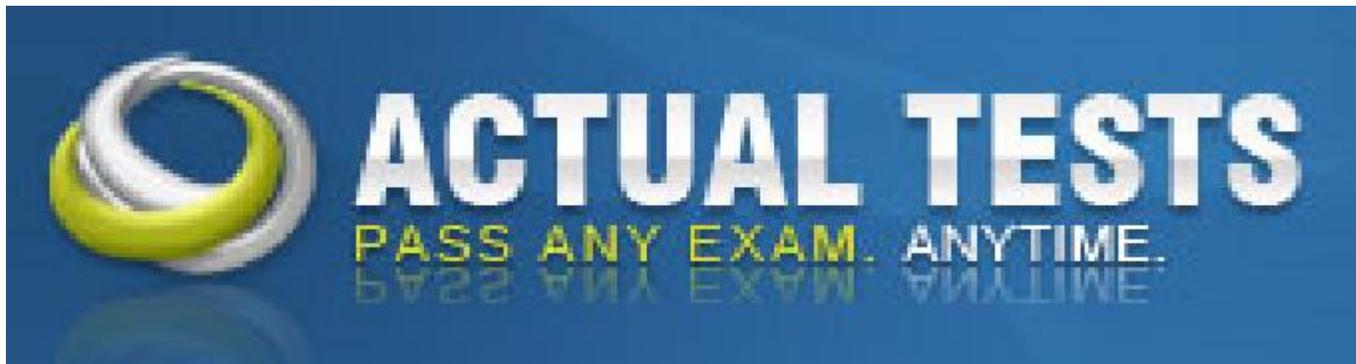


Microsoft.Actualtests.98-367.v2014-07-04.by.DAWN.24q

Number: 98-367
Passing Score: 700
Time Limit: 45 min
File Version: 14.5

Exam Code:98-367

Exam Name:Security Fundamentals



Certdumps

QUESTION 1

Your company maintains a Web server that is accessible to the public. It should be placed in a/an:

- A. primary DNS zone.
- B. enterprise domain.
- C. perimeter network.
- D. Virtual Private Network (VPN).

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

A network sniffer is software or hardware that:

- A. captures and analyzes network communication.
- B. records user activity and transmits it to the server.
- C. protects workstations from intrusions.
- D. catalogs network data to create a secure index.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

You are trying to establish communications between a client computer and server. The server is not responding. You confirm that both the client and the server have network connectivity.

Which should you check next?

- A. Data Execution Prevention
- B. Microsoft Update

- C. Active Directory Domains and Trusts
- D. Windows Firewall

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

The primary purpose of Network Access Protection (NAP) is to prevent:

- A. loss of data from client computers on a network.
- B. non-compliant systems from connecting to a network.
- C. unauthorized users from accessing a network.
- D. users on a network from installing software.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Which three file system objects can you specify the NTFS permissions for? (Choose three.)

- A. Parents
- B. Folders
- C. Extensions
- D. Files
- E. Subfolders

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

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. Advanced Encryption Standard (AES)
- B. Folder level permissions
- C. File-level permissions
- D. Distributed File System (DFS)
- E. BitLocker

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Which displays a user's level of access to a particular file or folder on the server?

- A. The Resultant Set of Policy
- B. The object's Effective Permission
- C. The client computer's registry
- D. The object's Advanced Attributes

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Biometrics are used to:

- A. study hacking behavior.
- B. perform security audits.
- C. authenticate users.

D. measure the attack surface.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

A group of users has access to Folder A and all of its contents. You need to prevent some of the users from accessing a subfolder inside Folder A.

- A. Disable folder sharing
- B. Change the owner
- C. Block inheritance
- D. Hide the folder

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

How can you confirm whether a computer on your network is the target of a brute force attack?

- A. Run the show all access command
- B. Use antivirus software to scan the computer
- C. Check your Windows folder for unsigned files
- D. Check the security log for failed authentication attempts

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

The default password length for a Windows Server domain controller is:

- A. 0.
- B. 5.
- C. 7.
- D. 14.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which is the minimum requirements to create BitLocker To Go media on a client computer?

- A. Windows Vista Enterprise Edition
- B. Windows 2000 Professional Service Pack 4
- C. Windows 7 Enterprise Edition
- D. Windows XP Professional Service Pack 3

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

You need to be able to track file access.

Which type of auditing should you implement?

- A. Object access
- B. Process tracking
- C. Directory services
- D. Logon events

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

Many Internet sites that you visit require a user name and password.

How should you secure these passwords?

- A. Reuse the same password
- B. Save them to a text file
- C. Enable session caching
- D. Save them to an encrypted file
- E. Configure the browser to save passwords

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

You receive a phone call. The caller tells you that your Internet Service Provider account has a problem. The caller asks you to provide you account's user name and password in order to fix the problem.

- A. social engineering.
- B. password spoofing.
- C. best practices.
- D. social networking.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Media Access Control (MAC) filtering enables you to:

- A. limit access to a network based on the client computer's network adapter.
- B. restrict communications to a specific Web site.
- C. prevent communications between specific IP addresses.
- D. set access permissions to a shared folder.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Which two vulnerabilities is a wireless network client exposed to? (Choose two.)

- A. Eavesdropping
- B. File corruption
- C. Rogue access points
- D. Buffer overflow

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

Which two security settings can be controlled by using group policy? (Choose two.)

- A. Access to the **Run...** command
- B. Automatic file locking
- C. Encrypted access from a smart phone
- D. Password complexity

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

You are a network administrator. All computers run Internet Explorer 8. You need to protect users from phishing.

Which should you enforce?

- A. Cross-Site Scripting Filter
- B. Antivirus protection
- C. InPrivate Browsing
- D. SmartScreen Filter

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

- A. disable copy and paste.
- B. lock the computer cases.
- C. apply a group policy.
- D. store media in a locked room.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

What is the primary advantage of using Active Directory Integrated Zones?

- A. Secure replication
- B. Password protection

- C. Non-repudiation
- D. Zone encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

The purpose of User Account Control (UAC) is to:

- A. limit the privileges of software.
- B. encrypt the user's account.
- C. secure your data from corruption.
- D. facilitate Internet Filtering.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

You need to restrict a domain account from accessing the Control Panel.

Which should you use?

- A. Domain Users and Groups
- B. Local group policy
- C. Local Users and Groups
- D. Group Policy Objects

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Phishing is an attempt to:

- A. limit access to e-mail systems by authorized users.
- B. corrupt e-mail databases through the use of viruses.
- C. steal data through the use of network intrusion.
- D. obtain information by posing as a trustworthy entity.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference: