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.geekcert.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

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 2

Which of the following can be used to implement two-factor authentications? Each correct answer represents a complete solution. Choose all that apply.

A. Firewall security rule

B. Password

C. Smart card

D. Encrypted network configuration

Correct Answer: BC

Answer: C and B

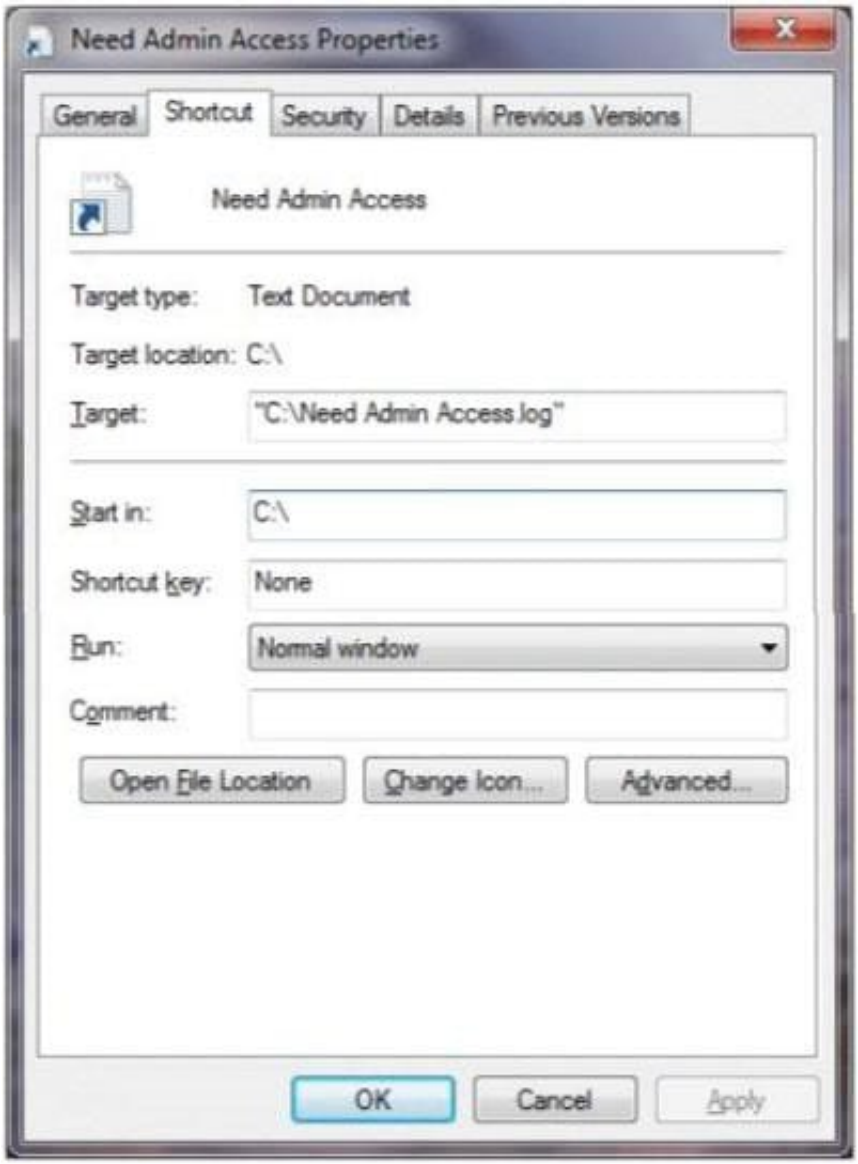
Two-factor authentication is defined as a security process that is used to confirm user identities by using two individual factors as follows:

Something they have such as token, smart cards, etc Something they know such as password.

QUESTION 3

You are at school and logged in to a Windows 7 computer using a standard user account.

You need to change some of the properties of a desktop icon for an assignment. Your instructor provides you with an administrator username and password and asks you to do two tasks.



When you open the Need Admin Access Properties window, you see the following image:

Use the drop-down menus to select the answer choice that completes each statement. Each correct selection is worth one point.

Hot Area:

Answer Area

To allow this log file to be opened as an administrator, you should **[answer choice]**

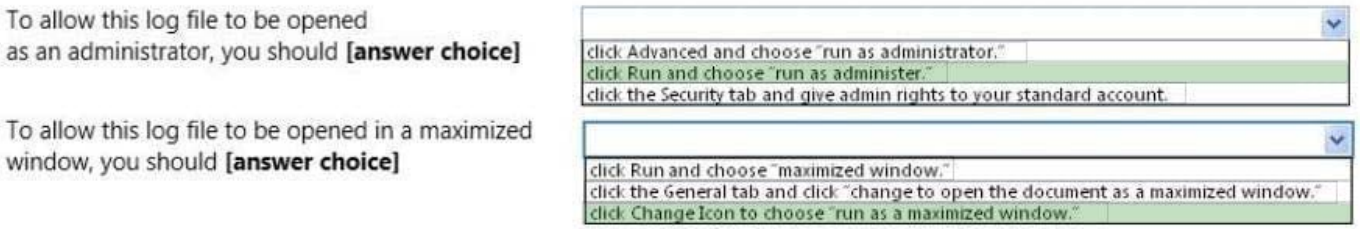
- click Advanced and choose "run as administrator."
- click Run and choose "run as administer."
- click the Security tab and give admin rights to your standard account.

To allow this log file to be opened in a maximized window, you should **[answer choice]**

- click Run and choose "maximized window."
- click the General tab and click "change to open the document as a maximized window."
- click Change Icon to choose "run as a maximized window."

Correct Answer:

Answer Area



QUESTION 4

Which of the following viruses cannot be detected by signature-based antivirus?

A. Macro virus

B. Boot sector virus

C. MBR virus

D. Polymorphic virus

Correct Answer: D

A polymorphic virus has the ability to change its own signature at the time of infection. This virus is very complicated and hard to detect. When the user runs the infected file in the disk, it loads the virus into the RAM. The new virus starts making its own copies and infects other files of the operating system. The mutation engine of the polymorphic virus generates a new encrypted code, thus changing the signature of the virus. Therefore, polymorphic viruses cannot be detected by signature-based antivirus. Answer: A is incorrect. A macro virus is a virus that consists of a macro code which infects the system. A Macro virus can infect a system rapidly. Since this virus has VB event handlers, it is dynamic in nature and displays random activation. The victim has only to open a file having a macro virus in order to infect the system with the virus. DMV, Nuclear, and Word Concept are some good examples of macro viruses. Answer: C is incorrect. A Master boot record (MBR) virus replaces the boot sector data with its own malicious code. Every time when the computer starts up, the boot sector virus executes. It can then generate activity that is either annoying (system will play sounds at certain times) or destructive (erase the hard drive of the system). Because the code in the Master Boot Record executes before any operating system is started, no operating system can detect or recover from corruption of the Master Boot Record. Answer: B is incorrect. A boot sector virus infects the master boot files of the hard disk or floppy disk. Boot record programs are responsible for booting the operating system and the boot sector virus copies these programs into another part of the hard disk or overwrites these files. Therefore, when the floppy or the hard disk boots, the virus infects the computer.

QUESTION 5

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 will Mark ask to employees of his company to do when they receive an email from a company they know with a request to click the link to "verify their account information"?

A. Provide the required information

B. Hide the email

C. Use Read-only Domain Controller

D. Delete the email

Correct Answer: D

In the above scenario, Mark will ask his employees to delete the email whenever he receives an email from a company that they know with to click the link to "verify their account information", because companies do not ask for account

information via email now a days.

Answer: C 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.