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

QUESTION 1

You have a new computer and want to restrict other people from replacing the operating system.

Which action prevents a user from installing an alternate operating system by using physical media if the user has physical media if the user has physical access to the computer?

A. installing drive-level encryption

B. disabling removable devices and drives

C. password protecting the computer BIOS

D. removing the user from the administrators group

Correct Answer: B

QUESTION 2

E-mail bombing attacks a specific entity by:

A. Redirecting all e-mail to another entity

B. Sending high volumes of e-mail

C. Tracing e-mail to the destination address

D. Triggering high levels of security alerts

Correct Answer: B

In Internet usage, an email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

QUESTION 3

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 4

Which of the following is a program that runs at a specific date and time to cause unwanted and unauthorized functions?

A. Keylogger

B. Logic bomb

C. Spyware

D. Trojan horse

Correct Answer: B

A logic bomb is a malicious program that executes when a predetermined event occurs. For example, a logic bomb can execute when a user logs on to a computer or presses certain keys on the keyboard. It can also execute on a particular

date or time specified by developers.

Answer: D is incorrect. Trojan horse is a malicious software program code that masquerades itself as a normal program. When a Trojan horse program is run, its hidden code runs to destroy or scramble data on the hard disk. An example of a

Trojan horse is a program that masquerades as a computer logon to retrieve user names and password information. The developer of a Trojan horse can use this information later to gain unauthorized access to computers. Trojan horses are

normally spread by e-mail attachments. Unlike viruses, Trojan horses do not replicate themselves but only destroy information on hard disks. Answer: A is incorrect. A keylogger is a software tool that traces all or specific activities of a user on

a computer. Once a keylogger is installed on a victim\\'s computer, it can be used for recording all keystrokes on the victim\\'s computer in a predefined log file. An attacker can configure a log file in such a manner that it can be sent

automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:

It can record all keystrokes.

It can capture all screenshots.

It can record all instant messenger conversations. It can be remotely installed.

It can be delivered via FTP or e-mail.

Answer: C is incorrect. Spyware is a computer program that collects all the information on the computer user and sends it to another computer or destination. It is used for monetary gain. It may have several ways of making money by using

the information obtained. It tries to violate the privacy of the computer without causing damage to the computer or the software installed on it.

QUESTION 5

You are trying to establish communications between a client computer and a server. The server is not responding.

You confirm that both the client and the server have network connectivity.

Which should you check next?

A. Microsoft Update

B. Data Execution Prevention

C. Windows Firewall

D. Active Directory Domains and Trusts

Correct Answer: D