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

Which of the following is a method of capturing and recording computer users\\' keystrokes including sensitive passwords?

A. Using hardware keyloggers

B. Using Alchemy Remote Executor

C. Using SocketShield

D. Using Anti-virus software

Correct Answer: A

Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users\\' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged

inline between a computer keyboard and

a computer. They log all keyboard activities to their internal memory. Answer: D is incorrect. Anti-Virus software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also

prevent and remove adware, spyware, and other forms of malware.

Anti-Virus software is a class of program that searches your hard drive, floppy drive, and pen drive for any known or potential viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the

Internet by businesses concerned about protecting their computer assets. Popular Anti-Virus packages are as follows: Bit Defender Anti-Virus McAfee Virus Scan Kaspersky Anti-Virus F-Secure Anti-Virus Symantec Norton Anti-Virus Panda

Titanium Anti-Virus Avira Anti-Virus Avast Anti-Virus Trend Micro Anti-Virus Grisoft AVG Anti-Virus ESET Nod32 Anti-Virus Webroot Anti-Virus Quick Heal Anti-Virus eTrust EZ Anti-Virus ZoneAlarm Anti-Virus

Answer: B is incorrect. Alchemy Remote Executor is a system management tool that allows Network Administrators to execute programs on remote network computers without leaving their workplace. From the hacker\\'s point of view, it can be

useful for installing keyloggers, spyware, Trojans, Windows rootkits and such. One necessary condition for using the Alchemy Remote Executor is that the user/attacker must have the administrative passwords of the remote computers on

which the malware is to be installed.

Answer: C is incorrect. SocketShield provides a protection shield to a computer system against malware, viruses, spyware, and various types of keyloggers. SocketShield provides protection at the following two levels:

1.Blocking: In this level, SocketShield uses a list of IP addresses that are known as purveyor of exploits. All http requests for any page in these domains are simply blocked.

2.Shielding: In this level, SocketShield blocks all the current and past IP addresses that are the cause of unauthorized access.

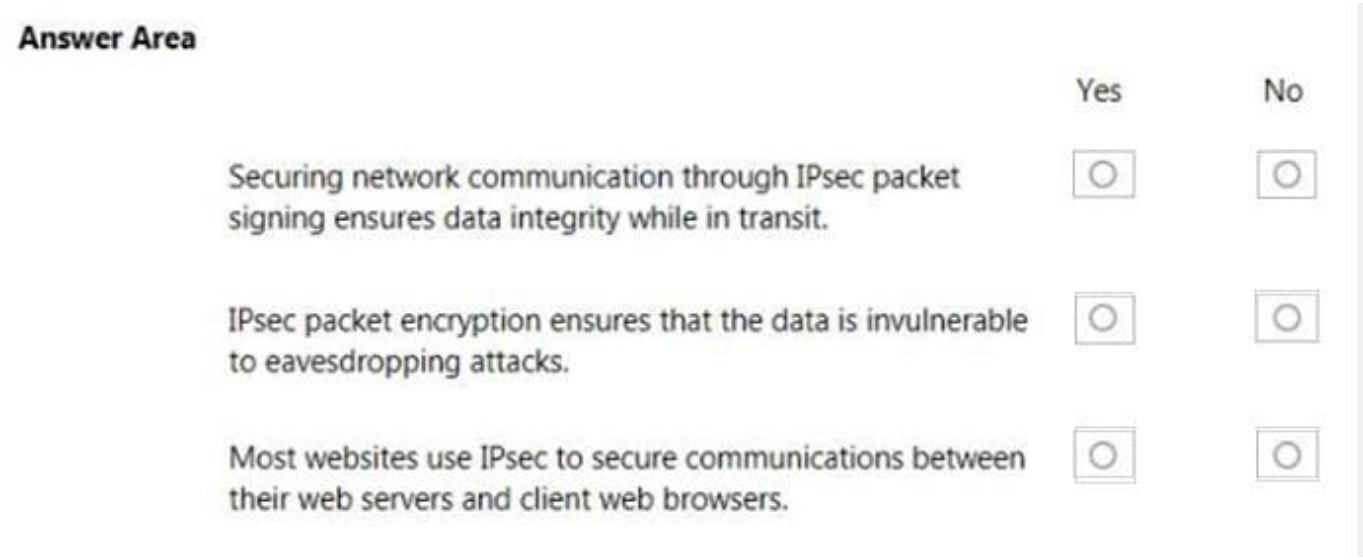
QUESTION 2

You are configuring the network settings of computers in your school\\'s computer lab.

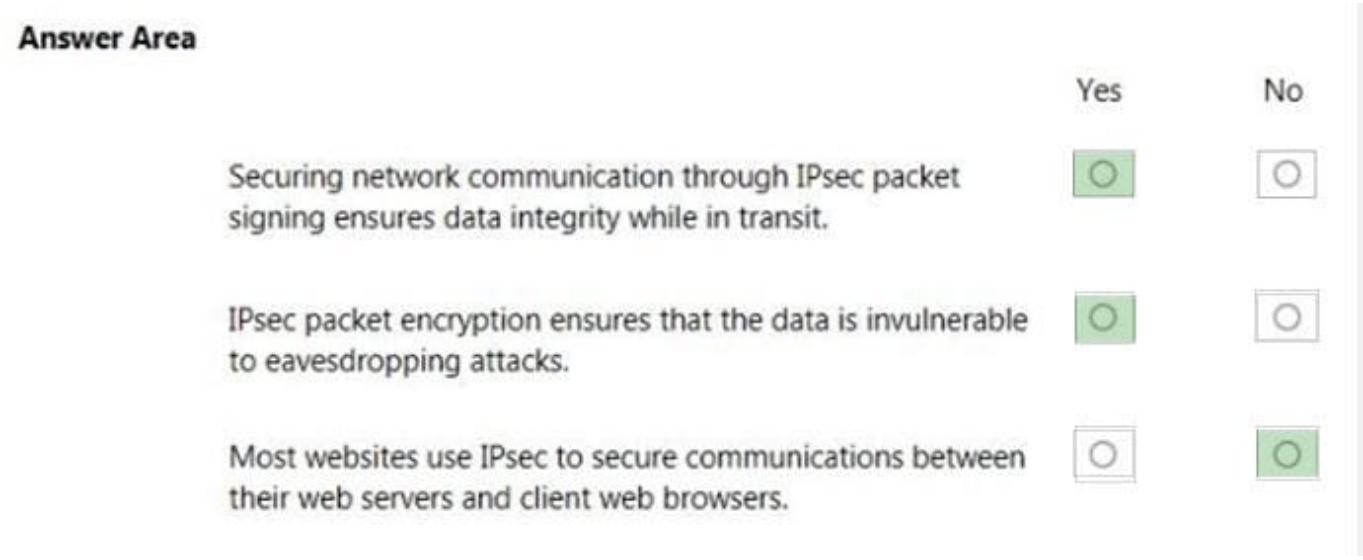
Instructions: For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



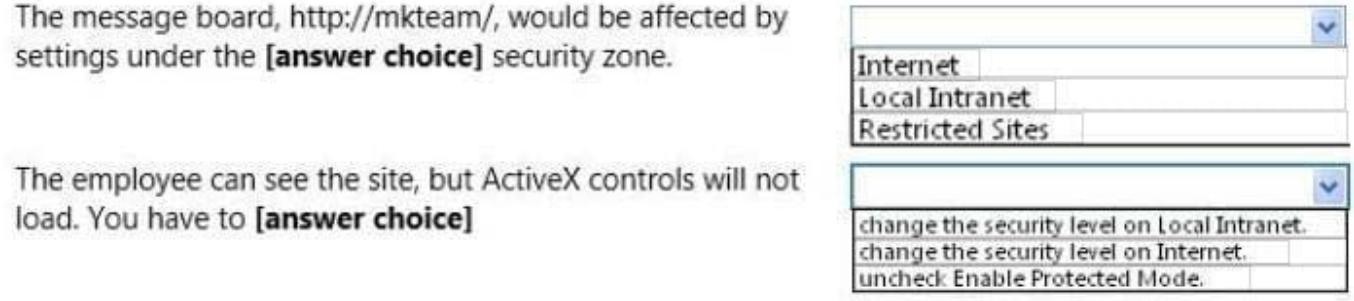
QUESTION 3

An employee where you work is unable to access the company message board in Internet Explorer. You review her Internet Options dialog box, as shown in the following image:

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

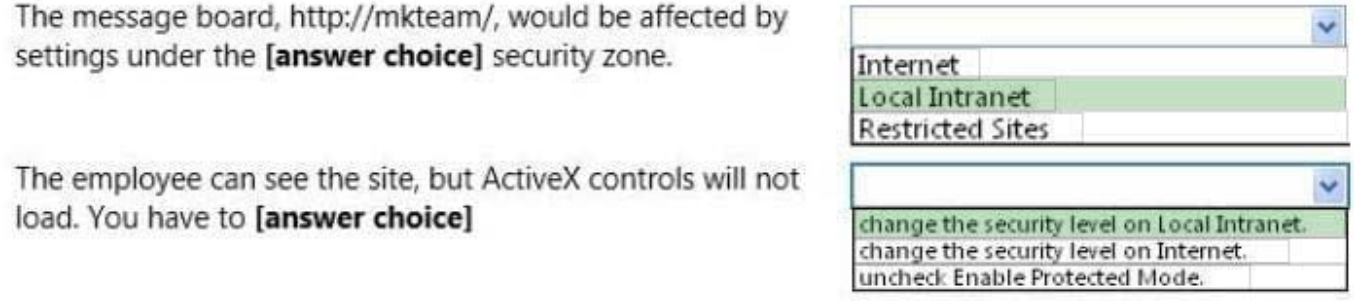
Hot Area:

Answer Area



Correct Answer:

Answer Area



QUESTION 4

Which of the following is the most common method for an attacker to spoof email?

A. Back door

B. Replay attack

C. Man-in-the-middle attack

D. Open relay

Correct Answer: D

An open relay is the most common method for an attacker to spoof email. An open relay is an SMTP mail server configured in such a way that it allows anyone on the Internet to send e-mail through it. By processing mail that is neither for nor from a local user, an open relay makes it possible for a spammer to route large volumes of spam. Answer: C is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer: A is incorrect. A backdoor is a program or account that allows access to a system by skipping the security checks. Many vendors and developers implement backdoors to save time and effort by skipping the security

checks while troubleshooting. A backdoor is considered to be a security threat and should be kept with the highest security. If a backdoor becomes known to attackers and malicious users, they can use it to exploit the system. Answer: B is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet.

QUESTION 5

Encrypting a hard disk is an example of ensuring:

A. security be default

B. confidentially

C. integrity

D. least privilege

Correct Answer: B