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.pass4itsure.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

Network Access Protection (NAP) enables administrators to control access to network resources based on a computer\\'s:

A. Encryption level

B. Warranty

C. Physical location

D. Configuration

Correct Answer: D

Network Access Protection (NAP) is a new set of operating system components included with the Windows Server?2008 and Windows Vista?operating systems that provides a platform to help ensure that client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer\\'s operating system and critical software. For example, computers might be required to have antivirus software with the latest signatures installed, current operating system updates installed, and a host-based firewall enabled. By enforcing compliance with health requirements, NAP can help network administrators mitigate some of the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software.

QUESTION 2

John works as a Network Administrator for We-are-secure Inc. The We-are-secure server is based on Windows Server 2003. One day, while analyzing the network security, he receives an error message that Kernel32.exe is encountering a problem. Which of the following steps should John take as a countermeasure to this situation? Each correct answer represents a complete solution. Choose all that apply.

A. He should restore his Windows settings.

B. He should upgrade his antivirus program.

C. He should observe the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new malicious process is running, he should kill that process.

D. He should download the latest patches for Windows Server 2003 from the Microsoft site, so that he can repair the kernel.

Correct Answer: BC

Answer: B and C

In such a situation, when John receives an error message revealing that Kernel32.exe is encountering a problem, he needs to come to the conclusion that his antivirus program needs to be updated, because Kernel32.exe is not a Microsoft

file (It is a Kernel32.DLL file.).

Although such viruses normally run on stealth mode, he should examine the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new process (malicious) is running on the server, he

should exterminate that process.

Answer: A and D are incorrect. Since kernel.exe is not a real kernel file of Windows, there is no need to repair or download any patch for Windows Server 2003 from the Microsoft site to repair the kernel.

Note: Such error messages can be received if the computer is infected with malware, such as Worm_Badtrans.b, Backdoor.G_Door, Glacier Backdoor, Win32.Badtrans.29020, etc.

QUESTION 3

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

QUESTION 4

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

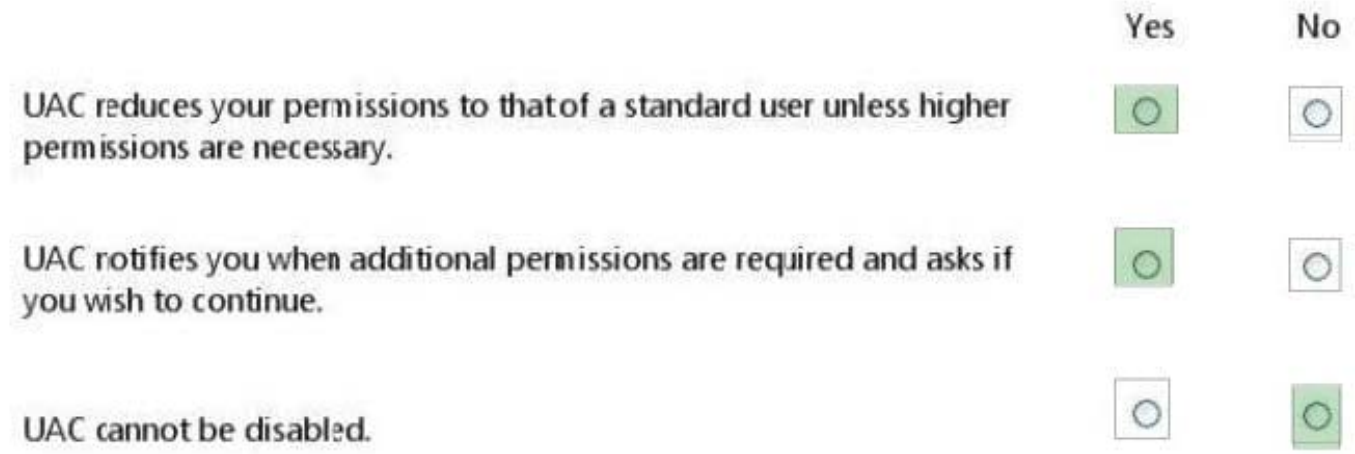
Hot Area:

Answer Area

	Yes	No
UAC reduces your permissions to thatof a standard user unless higher permissions are necessary.	○	○
UAC notifies you when additional permissions are required and asks if you wish to continue.	○	○
UAC cannot be disabled.	○	○

Correct Answer:

Answer Area



QUESTION 5

Which of the following is a security protocol that is used to protect data from being modified, corrupted, or accessed without authorization?

A. Honeypot

B. IP Security (IPsec)

C. DNSSEC

D. Protocol spoofing

Correct Answer: B

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. Answer: C is incorrect. Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. Answer: A is incorrect. A honey pot is a computer that is used to attract potential intruders or attackers. It is for this reason that a honey pot has low security permissions. A honey pot is used to gain information about the intruders and their attack strategies. Answer: D is incorrect. Protocol spoofing is used in data communications for enhancing the performance in situations where an currently working protocol is inadequate. In a computer security context, it refers to several forms of falsification of technically unrelated data.