Exam Report: 7.13.8 Practice Questions

Date: 1/23/2020 3:12:05 pm
Time Spent: 7:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 83%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following are disadvantages to server virtualization?

- Systems are isolated from each other and cannot interact with other systems
- Increased hardware costs
- A compromised host system might affect multiple servers
- A compromised guest system might affect multiple servers

Explanation

Virtualization allows a single physical machine (known as the *host* operating system) to run multiple virtual machines (known as the *guest* operating systems). The virtual machines appear to be self-contained and autonomous systems. Disadvantages of virtualization include:

- An attack on the host machine could compromise all guest machines operating on that host.
- A bottleneck or failure of any hardware component that is shared between multiple guests, such as a failure in a disk subsystem, could affect multiple virtual machines.
- While administration is centralized, virtualization is a newer technology and requires new skills, and managing virtual servers could add complexity.

A compromise of a guest system is typically limited to that system only because each virtual machine is kept partitioned from other guest machines. System isolation, if configured, is an advantage of virtualization. Isolation is typically used for testing purposes and prevents unreliable applications from interfering with other systems. Virtual systems do not need to be isolated; they can be configured to have full network access to other virtual machines or other network devices.

An advantage of virtualization is reduced hardware costs.

References

LabSim for Security Pro, Section 7.13.
[All Questions SecPro2017_v6.exm HOST_VIRT_01]

Question 2: Correct

Which of the following are disadvantages of server virtualization?

- Systems are isolated from each other and cannot interact with other systems.
- A failure in one hardware component could affect multiple servers.
- A compromise of a guest system might affect multiple servers.
- Increased hardware costs.

Explanation

Virtualization allows a single physical machine (known as the *host* operating system) to run multiple

virtual machines (known as the *guest* operating systems). The virtual machines appear to be self-contained and autonomous systems. Disadvantages of virtualization include:

- An attack on the host machine could compromise all guest machines operating on that host.
- A bottleneck or failure of any hardware component that is shared between multiple guests, such as a failure in a disk subsystem, could affect multiple virtual machines.
- While administration is centralized, virtualization is a newer technology and requires new skills, and managing virtual servers could add complexity.

A compromise of a guest system is typically limited to that system only because each virtual machine is partitioned from other guest machines. System isolation, if configured, is an advantage of virtualization. Isolation is typically used for testing purposes and prevents unreliable applications from interfering with other systems. Virtual systems do not need to be isolated; they can be configured to have full network access to other virtual machines or other network devices.

An advantage of virtualization is reduced hardware costs.

References

LabSim for Security Pro, Section 7.13.
[All Questions SecPro2017_v6.exm HOST_VIRT_02]

Question 3: Correct

You have a development machine that contains sensitive information relative to your business. You are concerned that spyware and malware might be installed while users browse websites, which could compromise your system or pose a confidentiality risk.

Which of the following actions would best protect your system?

- (•) Run the browser within a virtual environment
- ( ) Configure the browser to block all cookies and pop-ups
- ( ) Run the browser in protected mode
- ( ) Change the security level for the internet zone to High

Explanation

To best protect your system, run the browser in a virtual environment. Virtualization creates an environment that is logically separated from the main system. Any problems that occur within the virtual environment are contained within that environment and do not affect the rest of the system.

References

LabSim for Security Pro, Section 7.13.
[All Questions SecPro2017_v6.exm HOST_VIRT_03]

Question 4: Correct

Which of the following is an advantage of a virtual browser?

- ( ) Prevents phishing and drive-by downloads
- ( ) Filters internet content based on ratings
- ( ) Prevents adware and spyware that monitors your internet activity
- (•) Protects the host operating system from malicious downloads

Explanation

A virtual browser operates within a security sandbox that keeps activities within the browser from affecting the rest of the system. For example, malware downloaded by the virtual browser is limited to security sandbox and cannot harm the operating system.

The virtual browser does not prevent adware, spyware, or phishing; these threats are still possible within the virtual browser. However, if malware is installed within the virtual session, the malware cannot harm the rest of the system, and the virtual browser can be easily restored to remove the malicious software.

References

LabSim for Security Pro, Section 7.13.
[All Questions SecPro2017_v6.exm HOST_VIRT_04]

Question 5: Incorrect

Which of the following are advantages of virtualization? (Select two.)

- [x] ~~Reduced utilization of hardware resources~~
- [ ] Redundancy of hardware components for fault tolerance
- [x] Centralized administration
- [ ] Improved host-based attack detection
- [ ] Easy migration of systems to different hardware

Explanation

Virtualization allows a single physical machine (known as the *host* operating system) to run multiple virtual machines (known as the *guest* operating systems). The virtual machines appear to be self-contained and autonomous systems. Advantages of virtualization include:

- Server consolidation
- The ability to migrate systems between different hardware
- Centralized management of multiple systems
- Increase utilization of hardware resources
- Isolation of systems and applications

Disadvantages of virtualization include:

- A compromise in the host system could affect multiple guest systems
- A failure in a shared hardware resource could affect multiple systems

References

LabSim for Security Pro, Section 7.13.
[All Questions SecPro2017_v6.exm HOST_VIRT_05]

Question 6: Correct

Match the virtualization feature on the right with the appropriate description on the left.

Flexibility
- Moving virtual machines between hypervisor hosts

Testing
- Verifying that security controls are working as designed

Server consolidation
- Performing a physical-to-virtual migration (P2V)

Sandboxing
- Isolating a virtual machine from the physical network.

Explanation

Some of the advantages and features of virtualization include the following:

- **Flexibility**: Because they are self-contained, virtual machines can be easily moved between hypervisor hosts as needed.
- **Testing**: Virtual machines can be configured in a lab environment that mirrors your production network for testing purposes, such as testing security controls to verify that they are working as designed.
- **Server consolidation**: Server consolidation allows you to move physical systems onto just a few

hypervisors with many virtual machines. A physical-to-virtual migration (P2V) moves an operating system off physical hardware and into a virtual machine.

- **Isolation:** A sandboxed virtual machine is isolated from the physical network to allow testing without impacting the production environment.

References

LabSim for Security Pro, Section 7.13.
[All Questions SecPro2017_v6.exm HOST_VIRT_06]