Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/24/2022 8:36:21 pm • Time spent: 04:02

Score: 90% Passing Score: 80%

▼ Question 1: ✓ 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

9.1.3 Virtualization Facts

q_virt_browser_01_secp7.question.fex

▼ Question 2: ✓ Correct

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

○ Filters internet content based on ratings

○ Prevents phishing and drive-by downloads

○ Prevents adware and spyware that monitor 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 the 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

9.1.3 Virtualization Facts

q_virt_browser_02_secp7.question.fex

Question 3: ✓ Correct

Which of the following is an exploit in which malware allows the virtual OS to interact directly with the hypervisor?

- ○ Load balancing
- ➡ ● Escape
- ○ Jump
- ○ Bottleneck

EXPLANATION

Virtual machine escape is an exploit in which malware allows the operating system within a virtual machine to break out and interact directly with the hypervisor.

Jump is not a type of VM exploit.

Load balancing is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time.

A bottleneck is an area (software, hardware component, etc.) that all traffic slows down at.

REFERENCES

9.1.3 Virtualization Facts

q_virt_escape_secp7.question.fex

Question 4: ✓ Correct

Which of the following devices is computer software, firmware, or hardware that creates and runs virtual machines?

○ Virtual router

○ Virtual firewall

➡ ● Hypervisor

○ Virtual switch

EXPLANATION

A hypervisor is computer software, firmware, or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine. Each virtual machine is called a guest machine. The hypervisor provides the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems.

REFERENCES

9.1.3 Virtualization Facts

q_virt_hyper_secp7.question.fex

Question 5: ✓ Correct

Which of the following is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time?

➡ ● Load balancing

○ Bottleneck

○ Virtualization

○ Hypervisor

EXPLANATION

Load balancing is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time. The primary goal of load balancing is to improve performance and create high availability by configuring multiple devices to respond as one.

A hypervisor is a thin layer of software that resides between the guest operating system and the hardware.

Virtualization refers to installing and running multiple operating systems concurrently on a single physical machine.

A bottleneck is an area (software, hardware component, etc.) that all traffic slows down at.

REFERENCES

9.1.3 Virtualization Facts

q_virt_load_balance_secp7.question.fex

▾ Question 6: ✓ Correct

What is isolating a virtual machine from the physical network to allow testing to be performed without impacting the production environment called?

○ Workload balancing

○ Testing

➡ ● Sandboxing

○ Resource pooling

EXPLANATION

Isolating a virtual machine from the physical network to allow testing to be performed without impacting the production environment is known as sandboxing.

Resource pooling creates shared logical pools of CPU and memory resources from many physical machines within the hypervisor. This guarantees a level of resources for specific virtual machines.

Virtual machines can be configured in a lab environment that mirrors a production network to provide a testing environment.

Workload balancing distributes a workload (the total requests made by users and applications of a system) across multiple computers or a computer cluster to achieve optimal resource utilization, maximum throughput, minimal response time, and less overload.

REFERENCES

▷ 4.2.1 Operating System Hardening

4.2.2 Hardening Facts

4.2.3 Hardening an Operating System

4.2.4 Managing Automatic Updates

4.2.6 Configuring Microsoft Defender Firewall

4.2.8 Configuring Windows Defender with Firewall Advanced Security

9.1.3 Virtualization Facts

q_virt_sandbox_secp7.question.fex

Question 7: ✓ Correct

Which of the following are disadvantages of server virtualization?

○ A compromised guest system might affect multiple servers.

➡ ● A compromised host system might affect multiple servers.

○ It increases hardware costs.

○ Systems are isolated from each other and cannot interact with other systems.

EXPLANATION

Virtualization allows a single physical machine (known as the host operating system) to run multiple virtual machines (known as 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, so 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

9.1.3 Virtualization Facts

q_virt_server_secp7.question.fex

Question 8: ✓ Correct

Which type of hypervisor runs as an application on the host machine?

- ○ Type 3
- ○ Type 4
- ○ Type 1
- ➡ ● Type 2

EXPLANATION

A Type 2 hypervisor is known as a hosted hypervisor. It runs as an application on a conventional operating system.

A Type 1 hypervisor is like a thin operating system that directly interfaces with the computer hardware.

There are no Type 3 or Type 4 hypervisors.

REFERENCES

9.1.3 Virtualization Facts

q_virt_type2_secp7.question.fex

▼ **Question 9:** ✓ Correct

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

□ Improved host-based attack detection

➡ ☑ Easy migration of systems to different hardware

➡ ☑ Centralized administration

□ Reduced utilization of hardware resources

□ Redundancy of hardware components for fault tolerance

EXPLANATION

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

9.1.3 Virtualization Facts

q_virt_virtulize_secp7.question.fex

▼ Question 10: ✕ Incorrect

Which load balancing method distributes a workload across multiple computers?

- ○ Bottleneck
- ➡ ○ Workload balancing
- ○ Virtualization
- ● ~~Resource pooling~~

EXPLANATION

Workload balancing distributes a workload (the total requests made by users and applications of a system) across multiple computers or a computer cluster to achieve optimal resource utilization, maximum throughput, minimal response time, and less overload.

Resource pooling creates shared logical pools of CPU and memory resources from many physical machines within the hypervisor. This guarantees a level of resources for specific virtual machines.

Virtualization refers to installing and running multiple operating systems concurrently on a single physical machine.

A bottleneck is an area (software, hardware component, etc.) that all traffic slows down at.

REFERENCES

9.1.3 Virtualization Facts

q_virt_workload_secp7.question.fex