6.6.2 Module 6: Application Deployment and Security Quiz

itexamanswers.net/6-6-2-module-6-application-deployment-and-security-quiz.html

September 14, 2021

DevNet Associate 6.6.2 Module 6: Application Deployment and Security Quiz (Answers)

1. In serverless computing, which term refers to the ability for resources surrounding an app to change and adjust capacity as needed?

- extensible
- scalable
- **elastic**
- flexible

Explanation: In a serverless computing deployment model, the service provider provides resource capacity for customer applications. The resources and their capacity change as need changes and this is referred to as being elastic.

2. Which Linux-based platform is used to create, run, and manage containers in a virtual environment?

- **Docker**
- Hyper-V
- KVM
- Bash

Explanation: Container engines create, run, and manage containers. Docker is a very popular container engine.

3. What is Bash?

- **a Linux script engine that allows commands to be entered on the command line**
- a code injection technique used to attack data-driven applications
- a web application framework written in Python
- a philosophy for software deployment that figures prominently in the field of DevOps

Explanation: Bash is the name of a Linux script engine that lets a user do things from the command line. It is the default shell for most Linux distributions.

4. Which load balancing technique will check the load status of multiple hosting servers and send the next incoming request to the server with the lowest load?

- **least connections**
- IP hash
- canary
- blue-green

Explanation: In the least connections request servicing method, the load balancer will check the load status of multiple hosting servers and send the next incoming request to the lowest load server.

5. Which web application attack involves an attacker accessing, and potentially changing, serialized versions of data and objects?

- broken authentication
- **insecure deserialization**
- security misconfiguration
- cross-site scripting

Explanation: An insecure deserialization attack occurs when an attacker gains access to, and potentially changes, serialized versions of data and objects. This attack can be mitigated by ensuring validation before deserializing objects.

6. Which social engineering technique is carried out by someone attempting to gain access to a building by wearing a delivery service uniform?

- phishing
- **impersonation**
- vishing
- smishing

Explanation: Impersonation is a social engineering attack used to gain access to a system or network. Unlike other forms of social engineering attacks, impersonation occurs in person. The attacker impersonates someone whom others are likely to trust in an attempt to gain access to restricted resources.

7. A company has remote employees who need to connect to the company network in order to participate in meetings and to share the data and progress of application development. Which data transportation security technique can be implemented to allow remote employees to securely connect to the company private network?

- SSL
- SSH

- **VPN**
- TLS

Explanation: Data is vulnerable when it is transmitted over an insecure public network such as the internet. A company can use a virtual private network (VPN) to securely connect remote workers to the internal network and protect development and deployment resources as well as applications.

8. Which two attacks target web servers through exploiting possible vulnerabilities of input functions used by an application? (Choose two.)

- port scanning
- **SQL injection**
- trust exploitation
- **cross-site scripting**
- port redirection

Explanation: When a web application uses input fields to collect data from clients, threat actors may exploit possible vulnerabilities for entering malicious commands. The malicious commands that are executed through the web application might affect the OS on the web server. SQL injection and cross-site scripting are two different types of command injection attacks.

9. Which statement describes the term containers in virtualization technology?

- a group of VMs with identical OS and applications
- a subsection of a virtualization environment that contains one or more VMs
- isolated areas of a virtualization environment, where each area is administered by a customer
- **a virtual area with multiple independent applications sharing the host OS and hardware**

Explanation: In a virtualization environment, containers are a specialized "virtual area" where multiple applications can run independently of each other while sharing the same OS and hardware. By sharing the host operating system, most of the software resources are reused, which leads to reduced boot time and optimized operation.

10. A threat actor has used malicious commands to trick the database into returning unauthorized records and other data. Which web front-end vulnerability is the threat actor exploiting?

- security misconfiguration
- broken authentication
- **SQL injections**

- cross-site scripting

Explanation: Web front-end vulnerabilities apply to apps, APIs, and services. Some of the most significant vulnerabilities are as follows:

- **Cross-site scripting**: In a cross-site scripting (XSS) attack, the threat actor injects code, most often JavaScript, into the output of a web application. This forces client-side scripts to run the way that the threat actor wants them to run in the browser.
- **SQL injections**: In a SQLi the threat actor targets the SQL database itself, rather than the web browser. This allows the threat actor to control the application database.
- **Broken authentication**: Broken authentication includes both session management and protecting the identity of a user. A threat actor can hijack a session to assume the identity of a user especially when session tokens are left unexpired.
- **Security misconfiguration**: Security misconfiguration consists of several types of vulnerabilities all of which are centered on the lack of maintenance to the web application configuration.

11. What are three characteristics of a virtual machine? (Choose three.)

- **It includes a guest OS.**
- It leverages the kernel of the host OS for quick starts.
- **It is a virtualized physical server.**
- It shares the underlying resources of the host OS.
- It is an isolated environment for applications.
- **It requires a hypervisor.**

Explanation: A virtual machine is a software emulation of a physical server including a CPU, memory, network interface, and operating system. The hypervisor is virtualization software that performs hardware abstraction. It allows multiple VMs to run concurrently in the virtual environment.

12. What is a characteristic of the development environment in the four-tier deployment environment structure?

- **It is where coding takes place.**
- It is structurally similar to the final production environment.
- It is where users will interact with the code.
- It contains code that has been tested and is error free.

Explanation: There are four deployment environments: Development, testing, staging, and production. The first environment is the development environment which is where coding takes place.

13. What is CI/CD?

- It is a malicious code injection technique which is used to attack data-driven applications.
- It is a web application development framework that is written in Python.
- It is a script engine that allows users to execute commands from the command line.
- **It is a philosophy for software deployment that is often used in the field of DevOps.**

Explanation: CI/CD (continuous integration/continuous delivery) is a philosophy for software deployment that figures prominently in the field of DevOps.