Exam Report: 14.1.10 Practice Questions

Date: 5/26/2020 7:06:10 pm
Time Spent: 1:02

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 31%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

A company has subscribed to a cloud service that offers cloud applications and storage space. Through acquisition, the number of company employees quickly doubled. The cloud service vendor was able to add cloud services for these additional employees without requiring hardware changes. Which of the following cloud concepts does this represent?

- Resource pooling
- Rapid elasticity
- ~~On-demand service~~
- Measured service

Explanation

Rapid elasticity describes the cloud provider's ability to increase or decrease service levels to meet customer needs without requiring hardware changes.

Measured service refers to the way cloud services are measured or metered for billing purposes or according to a service level agreement.

An on-demand cloud service is available to users at any time.

Cloud service providers use resource pooling to supply services to multiple customers using shared physical resources.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_CLOUD_COMPUT_ADVANT_01_EH1]

Question 2: Incorrect

You are employed by a small start-up company. The company is in a small office and has several remote employees. You must find a business service that will accommodate the current size of the company and scale up as the company grows. The service needs to provide adequate storage as well as additional computing power. Which of the following cloud service models should you use?

- DaaS
- PaaS
- IaaS
- ~~SaaS~~

Explanation

Infrastructure as a Service (IaaS) delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing

servers, data center space, or network equipment.
Software as a Service (SaaS) delivers software applications to the client over the Internet or on a local area network.

Platform as a Service (PaaS) delivers everything a developer needs to build an application on the cloud infrastructure. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers.

Data as a Service (DaaS) stores and provides data from a centralized location without requiring local collection and storage.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_CLOUD_MODELS_01_EH1]

Question 3: Incorrect

Which of the following best describes the Platform as a Service (PaaS) cloud computing service model?

- Delivers software applications to the client either over the Internet or on a local area network.
- Delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments.
- ~~Stores and provides data from a centralized location, omitting the need for local collection and storage.~~
- Delivers everything a developer needs to build an application on the cloud infrastructure.

Explanation

Platform as a Service (PaaS) delivers everything a developer needs to build an application on the cloud infrastructure. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers.

Software as a Service (SaaS) delivers software applications to the client either over the Internet or on a local area network.

Infrastructure as a Service (IaaS) delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing servers, data center space, or network equipment.

Data as a Service (DaaS) stores and provides data from a centralized location, ommitting the need for local collection and storage.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_CLOUD_MODELS_02_EH1]

Question 4: Incorrect

Which of the following cloud computing service models delivers software applications to a client either over the Internet or on a local area network?

- DaaS
- ~~PaaS~~
- SaaS
- IaaS

Explanation

Software as a Service (SaaS) delivers software applications to the client either over the Internet or on a local area network.

Infrastructure as a Service (IaaS) delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing servers, data center space, or network equipment.

Platform as a Service (PaaS) delivers everything a developer needs to build an application on the cloud infrastructure. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers.

Data as a Service (DaaS) stores and provides data from a centralized location, omitting the need for local collection and storage.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_CLOUD_MODELS_03_EH1]

Question 5: Incorrect

Google Cloud, Amazon Web Services, and Microsoft Azure are some of the most widely used cloud storage solutions for enterprises. Which of the following factors prompts companies to take advantage of cloud storage?

- Need for a platform as a service for developing applications.
- Need for a storage provider to manage access control.
- Need to bring costs down and growing demand for storage.
- ~~Need for a software as a service to manage enterprise applications.~~

Explanation

Some of the most widely used cloud storage for enterprises are Google Cloud, Amazon Web Services, and Microsoft Azure. Because of the growing demand for storage and desire to bring costs down, many companies take advantage of cloud storage.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_CLOUD_MODELS_04_EH1]

Question 6: Correct

Strict supply chain management, comprehensive supplier assessment, HR resource requirements, transparent information security and management, compliance reporting, and a security breach notification process are defenses against which of the following cloud computing threats?

- Malicious insiders
- Multi-tenancy
- Data breach or loss
- Denial-of-service

Explanation

Malicious insiders are usually resentful people who have some kind of connection with a company or cloud service. The best defense is to have strict supply chain management, comprehensive supplier assessment, HR resource requirements, transparent information security and management, compliance reporting, and a security breach notification process.

Denial-of-service attacks are less likely to happen in a cloud environment, but they do occur. The best defense is to implement security best practices, monitor the environment for unauthorized activity, and secure authentication and access control.

Because resources are shared between clients, multi-tenancy can lead to data leakage or breach. Defend your data from this threat with end-to-end protection.

Data breach or loss happens when data is erased, changed, stolen, or lost. The best defense against this event is cloud data encryption, strong key generation, storage and management, proper design, and runtime protection for data.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing

[e_cloud_computing_eh1.exam.xml Q_CLOUD_THREATS_CLOUD_THREAT_FACTS_01_EH1]

Question 7: Incorrect

Which of the following is the best defense against cloud account and service traffic hijacking?

- Use physical security programs and have pre-installed standby hardware devices.
- Research risks, perform CSP due diligence, and use capable resources.
- ~~Use design and runtime protection for data, cloud data encryption, and strong key generation.~~
- Find and fix software flaws continuously, use strong passwords, and use encryption.

Explanation

Account and service traffic hijacking happens when the hacker exploits application weaknesses to take control of an account. The defenses are using strong passwords, using encryption, and finding and fixing software flaws continuously.

Poor security from lack of due diligence and understanding of content security policies in a cloud environment lead to successful attacks. The defenses are to research risks, use a content security policy, perform due diligence, and have capable resources.

Hardware failure makes cloud data inaccessible. Most failures happen because of hard disk malfunction. With that in mind, come up with a physical security program and keep it up to date.

Data breach or loss could happen in a few different ways. Data can be erased, changed, or decoupled. Encryption keys can be stolen or lost. Defenses are cloud data encryption; strong key generation, storage and management; and design and runtime protection for data.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_THREATS_CLOUD_THREAT_FACTS_02_EH1]

Question 8: Incorrect

A company has implemented the following defenses:

- The data center is located in safe geographical area.
- Backups are in different locations.
- Mitigation measures are in place.
- A disaster recovery plan is in place.

Which of the following cloud computing threats has the customer implemented countermeasures against?

- ~~Data breach or loss~~
- Denial-of-service
- Malicious insiders
- Natural disasters

Explanation

Natural disasters such as floods, lightning, and earthquakes can lead to service and data loss. Defenses are to locate data centers in a safe geographical area, have backups at different locations, take mitigation measures, and have a disaster recovery plan.

Denial-of-service attacks are less likely to happen in a cloud environment, but they still happen. Defenses are to implement security best practices, monitor the environment for unauthorized activity, and secure authentication and access control.

Malicious insiders are usually resentful people who have some kind of connection with a company or cloud service. Defenses are to have strict supply chain management, comprehensive supplier assessment, HR resources requirements, transparent information security and management, compliance reporting, and a security breach notification process.

Data breach or loss can happen in a few different ways. Data can be erased, changed, or decoupled. Encryption keys can be stolen or lost. Defenses are cloud data encryption; strong key generation, storage

and management; and design and runtime protection for data.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_THREATS_CLOUD_THREAT_FACTS_03_EH1]

Question 9: Correct

If an attacker's intent is to discover and then use sensitive data like passwords, session cookies, and other security configurations such as UDDI, SOAP, and WSDL, which of the following cloud computing attacks is he using?

- Session hijacking through session riding.
- Session hijacking through XSS attack.
- Service hijacking through social engineering.
- Service hijacking through network sniffing.

Explanation

When service hijacking through network sniffing, the attacker uses packet sniffers such as Wireshark or Cain and Abel to intercept and monitor traffic transmission between two cloud nodes. The attacker's intent is to discover and then user sensitive data such as passwords, session cookies, and other security configurations such as UDDI, SOAP, and WSDL.

Service hijacking through social engineering means the attacker uses approaches such as as pharming, phishing, and exploitation of software to steal a CSP's or client's credentials.

In an XSS attack, the hacker uses cross-site scripting to take the cookies utilized in the user authentication process.

In a session riding attack, the hacker rides an active computer session by tricking the user to visit a malicious website.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_ATTACKS_CLOUD_ATTACKS_FACTS_01_EH1]

Question 10: Incorrect

Which of the following best describes a cybersquatting cloud computing attack?

- The hacker runs a virtual machine on the physical host of a user's virtual machine in order to share physical resources.
- The hacker uses phishing scams by making a domain name that is almost the same as the cloud service provider.
- ~~The hacker discovers and uses sensitive data like passwords, session cookies, and other security configurations.~~
- The hacker sends the user to a fake website by poisoning the DNS server or cache on the user's system.

Explanation

When cybersquatting, the hacker uses phishing scams by making a domain name that is almost the same as the cloud service provider.

When using DNS poisoning, the hacker sends the user to a fake website by poisoning the DNS server or cache on the user's system.

When using side channel or cross-guest VM breaches, the hacker runs a virtual machine on the physical host of a user's virtual machine in order to share physical resources.
When using service hijacking through network sniffing, the hacker discovers and uses sensitive data like passwords, session cookies, and other security configurations.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_ATTACKS_CLOUD_ATTACKS_FACTS_02_EH1]

Question 11: Incorrect

You are using software as a service (SaaS) in your office. Who is responsible for the security of the data stored in the cloud?

- ~~The provider and the customer have no responsibility.~~
- The provider is responsible for all the security.
- The customer is responsible for all the security.
- The provider and the customer split responsibility.

Explanation

With software as a service (SaaS), the provider is supposed to provide all the security.

With infrastructure as a service (IaaS), you're responsible for pretty much every aspect of the security.

With platform as a service (PaaS), the security responsibility is split evenly between the cloud provider and the customer.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_SECURITY_CLOUD_SECURITY_FACTS_01_EH1]

Question 12: Correct

You are using BlazeMeter to test cloud security. Which of the following best describes BlazeMeter?

- A vulnerability scanner that can be used to detect viruses, malware, backdoors, and web services linking to malicious content.
- A load-testing tool for web and mobile applications that checks performance while the application is under a lot of traffic.
- An end-to-end performance and load testing tool that can simulate up to 1 million users and makes realistic load tests easier.
- An end-to-end security solution that assesses continually and is able to see all of your assets, no matter where they reside.

Explanation

BlazeMeter is an end-to-end performance and load testing tool that can simulate up to 1 million users and makes realistic load tests easier.

LoadStorm is a load-testing tool for web and mobile applications that checks performance while the application is under a lot of traffic.

Nexpose is a vulnerability scanner that can be used to detect viruses, malware, backdoors, and web services linking to malicious content.

Qualys Cloud Performa as an end-to-end security solution that assesses continually and is

able to see all of you assets, no matter where they reside.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_SECURITY_CLOUD_SECURITY_TOOLS_01_EH1]

Question 13: Correct

Which of the following cloud security controls includes backups, space availability, and continuity of services?

- Protecting information

- Administrative tasks
- Trusted computing
- Computation and storage

Explanation

With computation and storage, the cloud provider must have policies and procedures in place to protect data. These policies and procedures could include backups, space availability, and continuity of services.

The information layer protects information from being deleted, modified, or stolen.

Trusted computing involves computational environments that secure internal control, auditability, and maintenance.

The management layer involves all administrative tasks to promote continued, uninterrupted, and effective services.

References

TestOut Ethical Hacker Pro - 14.1 Cloud Computing
[e_cloud_computing_eh1.exam.xml Q_CLOUD_SECURITY_CLOUD_SECUR_CONTROL_01_EH1]