

## Review: Quiz 10 - Cloud Forensic (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points0.5 / 0.5 pts  
Auto-graded

1. When a hacker uses a compromised cloud account to attack additional accounts, they are leveraging the cloud as a tool. \*

☒ True ✓☐ False✓ **Correct** 0.5/0.5 Points0.5 / 0.5 pts  
Auto-graded

2. Which of the following best describes the cloud deployment model used for shared infrastructure among multiple enterprises with common concerns (e.g., security, compliance, jurisdiction)? \*

☐ Public Cloud☐ Private Cloud☒ Community Cloud ✓☐ Hybrid Cloud✓ **Correct** 0.5/0.5 Points0.5 / 0.5 pts  
Auto-graded

3. Cloud forensic investigations pose challenges related to multi-jurisdictional and multi-tenancy aspects. To better understand the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review? \*

☐ National and local regulation☒ Service level agreement ✓☐ Key performance indicator☐ Service level management

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

4. Which of the following terms is not associated with cloud forensics? \*

- ☐ eDiscovery
- ☐ Analysis
- ☒ Plausibility ✓
- ☐ Chain of custody

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

5. What is a concern for gathering forensics evidence in public cloud environments? \*

- ☐ High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.
- ☐ Configuration: Implementing security zones and proper network segmentation.
- ☐ Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.
- ☒ Multitenancy: Evidence gathering must avoid exposure of data from other tenants. ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

6. You work as a cloud security specialist at X Solutions. One of your clients is a healthcare organization that plans to migrate its electronic health record (EHR) system to the cloud. This system contains highly sensitive personal and medical data. As part of your job, you need to ensure the security and privacy of this data while it is being transferred and stored in the cloud. You recommend that the data be encrypted during transit and at rest. However, you also need to ensure that, even if a cloud service provider (CSP) has access to the encrypted data, they will not be able to decrypt it. Which of the following strategies would be the most suitable to meet this requirement? \*

- ☐ Rely on network-level encryption protocols for data transfer.
- ☐ Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.
- ☐ Utilize the CSP's built-in data encryption services.
- ☒ Use client-side encryption and manage encryption keys independently of the CSP. ✓

✓ **Correct** 0.5/0.5 Points0.5 / 0.5 pts  
Auto-graded

7. You are a security analyst for SkySec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements? \*

- ☐ Implement a Virtual Private Network (VPN) for secure data transmission.
- ☒ Deploy a Cloud Access Security Broker (CASB). ✓
- ☐ Use multi-factor authentication for all cloud user accounts.
- ☐ Use client-side encryption for all stored data.

✓ **Correct** 0.5/0.5 Points0.5 / 0.5 pts  
Auto-graded

8. As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software-as-a-Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment? \*

- ☐ Implement a Virtual Private Network (VPN) for accessing the SaaS applications.
- ☐ Rely on the cloud service provider's built-in security features.
- ☒ Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently. ✓
- ☐ Use multi-factor authentication for all user accounts accessing the SaaS applications

✓ **Correct** 0.5/0.5 Points0.5 / 0.5 pts  
Auto-graded

9. Alex, a cloud security engineer working at Eyecloud Inc., is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him develop, package, and run applications. Additionally, the technology provides PaaS through OS-level virtualization, delivers containerized software packages, and promotes fast software delivery \*

- ☐ Virtual machine
- ☒ Docker ✓
- ☐ Zero trust network
- ☐ Serverless computing

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

10. Why is it important to establish an agreement with a cloud provider before accessing cloud-based data for forensics? \*

- ☐ To ensure the data is safe from cyber threats
- ☒ To establish how the data should be shared and accessed (correct) ✓
- ☐ To determine the type of data being stored
- ☐ To determine the legal jurisdiction of the data

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

11. Which of the following tools allows you to create a snapshot of registry keys? (Choose all that apply) \*

- ☒ Regshot ✓
- ☒ WhatChanged ✓
- ☐ Wireshark
- ☐ RAM Capture

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

12. Which tool allows monitoring changes to the hard drive? (Choose all that apply) \*

- ☒ Disk Pulse ✓
- ☒ FolderChangesView ✓
- ☐ RAM Capture
- ☐ Disk Browser

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

13. What does the file C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive.Ink mean? \*

- ☒ Google Drive can be searched for in the Start Menu of Windows ✓
- ☐ Google Drive can autostart with Windows
- ☐ Google Drive has an error when installing on Windows

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

14. Which tool allows you to view the running process information of the Google Drive service? (Choose all that apply) \*

☒ Process Monitor ✓

☐ Disk Pulse

☒ Process Hacker ✓

☒ Process Explorer ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

15. By default, files in Google Drive's trash will be deleted after how many days? \*

30

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

16. With a free Google account, how many versions can a document store at most? \*

100

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

17. Which file in the DriveFS folder may contain information about the logged-in Google Drive account? \*

☐ parent.txt

☒ drive\_fs.txt ✓

☐ experiments.db

☐ root\_preference\_sqlite.db

☐ metric\_store\_sqlite.db

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

18. By default, on Windows 10 64-bit, where will Google Drive be installed? \*

- ☐ C:\Program Files\Microsoft\
- ☐ C:\Program Files\Oracle\
- ☐ C:\Program Files\Java
- ☒ C:\Program Files\Google\ ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

19. In the **Details** section, what information about the file can be viewed? (Choose all that apply) \*

- ☒ File owner ✓
- ☒ File type ✓
- ☐ File sharing expiration time
- ☒ File last modified ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts  
Auto-graded

20. After installing the latest version of the Google Drive software (100.0) on Windows 10, can we find information about some artifact files like **snapshot.db**? \*

- ☐ Yes
- ☒ No ✓