Western Governors University (WGU) C838 Managing Cloud Security (CCSP) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Questions

1. **An attacker establishes themselves on a system in such a way to enable the stealing of data over time. What kind of attack is this?**

   A. A Data Breach

   B. B Malicious Insider

   C. C Advanced Persistent Threats

   D. D Account Hijacking

2. **Which attack vector is associated with cloud infrastructure?**

   A. A Seizure and examination of a physical disk

   B. B Licensing fees tied to the deployment of software based on a per-CPU licensing model

   C. C Data storage locations in multiple jurisdictions

   D. D Compromised API credentials

3. **Which tool can help in isolating and analyzing attacks by luring potential attackers?**

   A. Firewall

   B. Honeypot

   C. Encryption module

   D. Network scanner

4. **Which controls does the STAR program rely on for cloud provider assessments?**

   A. CSA Cloud Controls Framework

   B. ISO 27001 Framework

   C. NIST Cybersecurity Framework

   D. COBIT Framework

5. **What type of BCDR (Business Continuity and Disaster Recovery) strategy involves the selection of an additional deployment zone and recreation of the processing capacity on a different location?**

   A. Data Replication

   B. Functionality Replication

   C. File Replication

   D. Database Replication

6. **How is redundancy achieved in virtual switches within a VLAN network?**
   - **A. Using port forwarding**
   - **B. Using port channeling**
   - **C. Using kernel-based virtual machine**
   - **D. Increasing network traffic**

7. **In which cloud environment scenario does the business continuity strategy restore the service failover to another part of the same CSP infrastructure?**
   - **A. Cloud service consumer, alternative provider BCDR**
   - **B. Cloud service consumer, primary provider BCDR**
   - **C. On-premises, cloud as BCDR**
   - **D. Cloud user, alternative BCDR cloud provider**

8. **What does vendor lock-out refer to in a cloud service context?**
   - **A. The inability to access support services**
   - **B. Losing access to data when a provider ceases operation**
   - **C. Restricted access to certain features**
   - **D. Increased costs associated with service changes**

9. **Which technology makes the network control programmable and dynamically adjusts the flow of traffic when the pattern of network consumption changes?**
   - **A. Application-defined networking**
   - **B. Network function virtualization**
   - **C. Hardware-defined networking**
   - **D. Software-defined networking**

10. **Which of the following is not a cloud deployment model?**
    - **A. Private**
    - **B. Public**
    - **C. Open**
    - **D. Hybrid**

Answers

1. **C**
2. **D**
3. **B**
4. **A**
5. **B**
6. **B**
7. **B**
8. **B**
9. **D**
10. **C**

Explanations

1. **An attacker establishes themselves on a system in such a way to enable the stealing of data over time. What kind of attack is this?**

   A. A Data Breach

   B. B Malicious Insider

   C. C Advanced Persistent Threats

   D. D Account Hijacking

The scenario described involves an attacker who embeds themselves in a system to gradually steal data over a prolonged period. This type of attack is characteristic of Advanced Persistent Threats (APTs). APTs typically involve a coordinated, sustained effort by attackers to gain and maintain access to a system, often through multiple strategies, including exploiting vulnerabilities, social engineering, or using malware. Once the attacker successfully gains access, they can then harvest sensitive data discreetly, evading immediate detection. This stealthy approach is a hallmark of APTs, distinguishing them from other attack types, which may be more opportunistic or limited in duration. The persistent nature of APTs implies ongoing surveillance and data extraction over time, as opposed to a single event, making this the most fitting description of the attack discussed in the question. APTs are often associated with well-resourced attackers, including organized cybercriminal groups or nation-state actors, who have the capacity and intent to engage in extended campaigns targeting valuable information.

2. **Which attack vector is associated with cloud infrastructure?**

   A. A Seizure and examination of a physical disk

   B. B Licensing fees tied to the deployment of software based on a per-CPU licensing model

   C. C Data storage locations in multiple jurisdictions

   D. D Compromised API credentials

The attack vector that is closely associated with cloud infrastructure is compromised API credentials. Application Programming Interfaces (APIs) are vital for interaction between different software systems, especially in cloud environments where services often communicate with each other over the internet. If an attacker gains access to valid API credentials, they can manipulate cloud resources, retrieve sensitive data, or even impact the availability of services without authorization. Compromised API credentials can lead to significant security incidents because cloud services rely heavily on APIs to enable functionalities, manage resources, and facilitate user interactions. Given that cloud environments are designed for ease of access and integration, a security breach in API authentication leads to potentially severe consequences. The other options do not directly relate to common attack vectors found in cloud infrastructure. The seizure of a physical disk refers to a more traditional attack vector occurring in on-premises environments. Licensing fees based on a per-CPU model pertain to software deployment practices rather than security concerns. Data storage across multiple jurisdictions involves legal complexities and compliance considerations but does not specifically denote an attack vector. Thus, compromised API credentials stand out as a direct threat to cloud infrastructure security.

3. Which tool can help in isolating and analyzing attacks by luring potential attackers?

A. Firewall

B. Honeypot

C. Encryption module

D. Network scanner

The correct choice identifies a honeypot as a tool designed specifically to lure potential attackers by simulating a vulnerable target. This is a strategic security measure that allows organizations to isolate and analyze malicious activities in a controlled environment. A honeypot appears to be an easy target, enticing attackers to engage with it, thus allowing security teams to monitor their techniques, gather threat intelligence, and understand the motives behind their actions without putting real assets at risk. In contrast, a firewall is primarily used to control incoming and outgoing network traffic based on predetermined security rules, but it does not facilitate the direct observation of attacker behavior in a manner that a honeypot does. An encryption module protects data by encoding it, making it unreadable to unauthorized users, rather than engaging actively with attackers. A network scanner is used to identify devices on a network and assess security vulnerabilities, but it doesn't serve the purpose of attracting attackers for analysis. Therefore, the honeypot stands out as the most effective tool for both isolating and analyzing attack methods.

4. Which controls does the STAR program rely on for cloud provider assessments?

A. CSA Cloud Controls Framework

B. ISO 27001 Framework

C. NIST Cybersecurity Framework

D. COBIT Framework

The STAR program, which stands for Security, Trust, Assurance, and Risk, is administered by the Cloud Security Alliance (CSA) and focuses on providing a framework for assessing and improving cloud security practices among cloud service providers. The CSA Cloud Controls Framework is specifically designed to address cloud-specific security controls and best practices. This framework includes a detailed set of security controls that cloud service providers can implement and assess, making it highly relevant for evaluating their security measures. By relying on this framework, the STAR program ensures that the assessments are aligned with the unique challenges and characteristics of cloud environments, promoting consistency and thoroughness in evaluating cloud security. The other frameworks, while important in their own rights, do not specifically cater to the needs of cloud environments in the same way the CSA Cloud Controls Framework does. ISO 27001, for example, is a broader information security management standard and while it can be applied in cloud contexts, it does not specifically address cloud-specific issues to the extent that the CSA framework does. Similarly, the NIST Cybersecurity Framework and COBIT Framework are valuable for overall security management and governance but do not focus on cloud-specific controls in the same structured manner as the CSA framework, making the CSA Cloud Controls Framework the appropriate choice for the STAR

5. What type of BCDR (Business Continuity and Disaster Recovery) strategy involves the selection of an additional deployment zone and recreation of the processing capacity on a different location?

A. Data Replication

B. Functionality Replication

C. File Replication

D. Database Replication

The strategy that involves the selection of an additional deployment zone and the recreation of processing capacity in a different location is functionality replication. This approach ensures that not only the data is backed up or mirrored at a secondary site, but the entire application or service's operational capability is also restored. This allows for continuous service delivery even if the primary site experiences a disaster or outage. Functionality replication ensures that the environment, including applications, configurations, and necessary resources, can be instantiated quickly at the alternative location, thereby minimizing downtime and maintaining business operations. On the other hand, data replication, file replication, and database replication primarily focus on duplicating data or specific types of information rather than recreating the entire operational capacity or service functionality in a new zone. Each of these alternatives typically involves different methodologies primarily centered around data preservation and retrieval rather than comprehensive service restoration.

6. How is redundancy achieved in virtual switches within a VLAN network?

A. Using port forwarding

B. Using port channeling

C. Using kernel-based virtual machine

D. Increasing network traffic

Redundancy in virtual switches within a VLAN (Virtual Local Area Network) network is effectively achieved through port channeling. Port channeling, also known as link aggregation, allows multiple physical network links to be combined into a single logical link. This approach not only increases bandwidth but also provides redundancy; if one of the physical links fails, traffic can continue to flow over the remaining links without disruption. By using port channeling, data packets can be sent over multiple paths, thereby enhancing fault tolerance. In the event of a network issue affecting one of the physical connections in the channel, the virtual switch can seamlessly use the operational connections to maintain network availability. This provides a robust solution to avoid single points of failure and ensures that the VLAN network can function reliably even under adverse conditions.

7. In which cloud environment scenario does the business continuity strategy restore the service failover to another part of the same CSP infrastructure?

A. Cloud service consumer, alternative provider BCDR

B. Cloud service consumer, primary provider BCDR

C. On-premises, cloud as BCDR

D. Cloud user, alternative BCDR cloud provider

The scenario where the business continuity strategy restores service failover to another part of the same cloud service provider (CSP) infrastructure is best represented by the situation where the cloud service consumer relies on the primary provider's Business Continuity and Disaster Recovery (BCDR) capabilities. In this context, a primary provider BCDR ensures that in the event of a service disruption, there are built-in mechanisms within the same CSP to reroute workloads, data, and services to another operational segment of the provider's infrastructure. This is crucial for maintaining service availability and minimizing downtime without requiring the consumer to seek external solutions or alternate providers. Using the same CSP allows for streamlined recovery processes and typically benefits from pre-configured strategies and resources that the provider already has in place, effectively managing risks and ensuring faster recovery times. This approach provides a more seamless transition during failovers compared to moving data and services to a different provider. The other scenarios involve different approaches to BCDR, such as relying on alternative providers or on-premises solutions, which may not leverage the existing infrastructure of the primary cloud provider as effectively for rapid recovery and continuity.

8. What does vendor lock-out refer to in a cloud service context?

A. The inability to access support services

B. Losing access to data when a provider ceases operation

C. Restricted access to certain features

D. Increased costs associated with service changes

Vendor lock-out in a cloud service context refers to the situation where a customer loses access to their data or service capabilities when a cloud service provider ceases operations. This scenario illustrates the potential risks associated with dependency on a single vendor, where the termination of service can disrupt access to critical data stored in that cloud environment. In this case, the customer might find it difficult or impossible to migrate their data to another platform, leading to significant operational challenges and possible data loss. Understanding this risk underscores the importance of having a robust data management strategy and considering exit strategies when selecting cloud services. This issue is prevalent among customers who have not thoroughly evaluated their service agreements or do not have contingency plans in place, highlighting the critical nature of awareness and planning in cloud service utilization.

9. Which technology makes the network control programmable and dynamically adjusts the flow of traffic when the pattern of network consumption changes?

A. Application-defined networking

B. Network function virtualization

C. Hardware-defined networking

D. Software-defined networking

Software-defined networking (SDN) is the correct answer because it allows for programmable network control. This technology separates the network control plane from the data plane, enabling administrators to manage network resources more flexibly and efficiently through software applications rather than relying on physical hardware configurations. With SDN, the management of network traffic flows can be adjusted dynamically in response to changing patterns in network consumption, facilitating optimal performance and resource allocation. The ability of SDN to abstract network functions and provide a centralized view of the network allows for rapid adjustments and improved agility. This adaptability is key in modern networking, particularly in environments where rapid changes in demand or traffic patterns occur frequently. SDN's programmable nature lets organizations implement changes quickly without the need for manual reconfiguration of physical devices, thus enhancing operational efficiency and responsiveness. In contrast, application-defined networking focuses on how applications interact with the network without necessarily providing the same level of control over network infrastructure itself. Network function virtualization, while it does virtualize network functions, does not inherently offer the programmability across the entire network that SDN does. Lastly, hardware-defined networking typically refers to traditional networking practices and does not incorporate the programmability aspect that is central to SDN's functionality.

10. Which of the following is not a cloud deployment model?

A. Private

B. Public

C. Open

D. Hybrid

The correct answer is "Open" because it is not recognized as a formal cloud deployment model within the frameworks established in cloud computing. The three established models of cloud deployment are private, public, and hybrid. A private cloud is designed for exclusive use by a single organization, allowing for greater control over resources and security. A public cloud is available to multiple entities and is owned and operated by third-party service providers, offering scalability and lower costs. A hybrid cloud combines elements of both private and public clouds, providing flexibility in data management and deployment strategies. "Open," while it may refer to principles of interoperability or open-source technologies used within cloud environments, does not stand as a distinct category of cloud deployment. This understanding clarifies why "Open" is the response that does not align with recognized cloud deployment models.