CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A company creates digitally signed packages for its devices. Which of the following best describes the method by which the security packages are delivered to the company\\'s customers?

A. Antitamper mechanism

B. SELinux

C. Trusted firmware updates

D. eFuse

Correct Answer: C

Trusted firmware updates are a method by which security package" customers. Trusted firmware updates are digitally signed packages that contain software updates or patches for devices, such as routers, switches, or firewalls. Trusted firmware updates can help to ensure the authenticity and integrity of the packages by verifying the digital signature of the sender and preventing unauthorized or malicious modifications to the packages . https://www.cisco.com/c/en/us/td/docs/ ios-xml/ios/sec_usr_trustsec/configuration/xe-16/sec-usr-trustsec-xe-16-book/sec-trust-firm-upd.html

QUESTION 2

A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:

Log entry #	Message
Log entry 1	comptia.org/${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='../index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

Which of the following log entries provides evidence of the attempted exploit?

A. Log entry 1

B. Log entry 2

C. Log entry 3

D. Log entry 4

Correct Answer: A

QUESTION 3

An organization wants to move non-essential services into a cloud computing environment. The management team has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work best to attain the desired outcome?

A. Duplicate all services in another instance and load balance between the instances.

B. Establish a hot site with active replication to another region within the same cloud provider.

C. Set up a warm disaster recovery site with the same cloud provider in a different region.

D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Correct Answer: C

Setting up a warm disaster recovery site with the same cloud provider in a different region can help to achieve a recovery time objective (RTO) of 12 hours while keeping the costs low. A warm disaster recovery site is a partially configured site that has some of the essential hardware and software components ready to be activated in case of a disaster. A warm site can provide faster recovery than a cold site, which has no preconfigured components, but lower costs than a hot site, which has fully configured and replicated components. Using the same cloud provider can help to simplify the migration and synchronization processes, while using a different region can help to avoid regional outages or disasters . https://www.techopedia.com/definition39/memory-dump

QUESTION 4

A security analyst observed the following activity from a privileged account:

Accessing emails and sensitive information Audit logs being modified Abnormal log-in times

Which of the following best describes the observed activity?

A. Irregular peer-to-peer communication

B. Unauthorized privileges

C. Rogue devices on the network

D. Insider attack

Correct Answer: D

Explanation: The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization\\'s reputation, operations, and compliance12. References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users\\' Activities in Active Directory

QUESTION 5

Given the output below:

#nmap 7.70 scan initiated Tues, Feb 8 12:34:56 2022 as: nmap -v -Pn -p 80,8000,443 --script http-* -oA server.out 192.168.220.42

Which of the following is being performed?

A. Cross-site scripting

B. Local file inclusion attack

C. Log4] check

D. Web server enumeration

Correct Answer: D

Web server enumeration is the process of identifying information about a web server, such as its software version, operating system, configuration, services, and vulnerabilities. This can be done using tools like Nmap, which can scan ports and run scripts to gather information. In this question, the Nmap command is using the -p option to scan ports 80, 8000, and 443, which are commonly used for web services. It is also using the --script option to run scripts that start with http-*, which are related to web server enumeration. The output file name server.out also suggests that the purpose of the scan is to enumerate web servers. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://partners.comptia.org/docs/defaultsource/ resources/comptia-cysa-cs0-002-exam-objectives