Vendor: CompTIA

Exam Code: CS0-002

Exam Name: CompTIA Cybersecurity Analyst (CySA+) Certification Exam

Version: 13.03

Q & As: 372

QUESTION 1
A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?

A. Implement IPSec rules on the application servers through a GPO that limits RDP access from only the jump host. Patch the jump host. Since it does not run the application natively, it will not affect the software's operation and functionality. Do not patch the application servers until the compatibility issue is resolved.
B. Implement IPSec rules on the jump host server through a GPO that limits RDP access from only the other application servers. Do not patch the jump host. Since it does not run the application natively, it is at less risk of being compromised. Patch the application servers to secure them.
C. Implement IPSec rules on the application servers through a GPO that limits RDP access to only other application servers. Do not patch the jump host. Since it does not run the application natively, it is at less risk of being compromised. Patch the application servers to secure them.
D. Implement firewall rules on the application servers through a GPO that limits RDP access to only other application servers. Manually check the jump host to see if it has been compromised. Patch the application servers to secure them.

Correct Answer: A

QUESTION 2
An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

A. Manually log in to the service and upload data files on a regular basis.
B. Have the internal development team script connectivity and file translate to the new service.
C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
D. Utilize the cloud products API for supported and ongoing integrations

Correct Answer: D

QUESTION 3
An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?

A. Data retention
B. Evidence retention
C. GDPR
D. Data correlation procedure

Correct Answer: A
QUESTION 4
Which of the following should a database administrator implement to BEST protect data from an

untrusted server administrator?

A. Data encryption
B. Data deidentification
C. Data masking
D. Data minimization

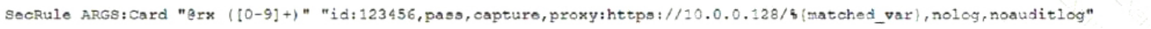
Correct Answer: A

QUESTION 5
A security analyst needs to reduce the overall attack surface. Which of the following infrastructure changes should the analyst recommend?

A. Implement a honeypot.
B. Air gap sensitive systems.
C. Increase the network segmentation.
D. Implement a cloud-based architecture.

Correct Answer: C

QUESTION 6
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts .conf file The output of the diff command against the known-good backup reads as follows



```
SecRule ARGS:Card "@rx ([0-9]+)" "id:123456,pass,capture,proxy:https://10.0.0.128/%{matched_var},nolog,noauditlog"
```

Which of the following MOST likely occurred?

A. The file was altered to accept payments without charging the cards
B. The file was altered to avoid logging credit card information
C. The file was altered to verify the card numbers are valid.
D. The file was altered to harvest credit card numbers

Correct Answer: A

QUESTION 7
A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics. cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

A. Cloning procedures
B. Chain of custody
C. Hashing procedures
D. Virtualization

Correct Answer: B

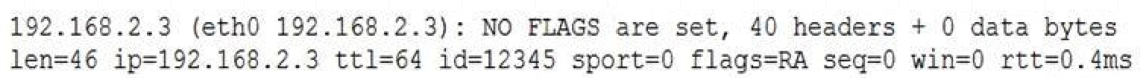
QUESTION 8
An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented. Which of the following methods would BEST secure the company's infrastructure and be the

simplest to manage and maintain?

A. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment.
B. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules.
C. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.
D. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account.

Correct Answer: C

QUESTION 9
An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization's network and identify active hosts. An analyst sees the following output from a packet capture:



```
192.168.2.3 (eth0 192.168.2.3): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.2.3 ttl=64 id=12345 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
```

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

A. flags=RA indicates the testing team is using a Christmas tree attack
B. ttl=64 indicates the testing team is setting the time to live below the firewall's threshold
C. 0 data bytes indicates the testing team is crafting empty ICMP packets
D. NO FLAGS are set indicates the testing team is using hping

Correct Answer: D

QUESTION 10
An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

A. Root-cause analysis
B. Active response
C. Advanced antivirus
D. Information-sharing community
E. Threat hunting

Correct Answer: E

QUESTION 11
A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

A. Open Source Security Information Management (OSSIM)
B. Software Assurance Maturity Model (SAMM)
C. Open Web Application Security Project (OWASP)