Vendor: CompTIA

Exam Code:SY0-601

Exam Name: CompTIA Security+

Version: Demo

QUESTION 1

A security analyst is working with a vendor to get a new SaaS application deployed to an enterprise. The analyst wants to ensure role-based security policies are correctly applied as users access the application. Which of the following is most likely to solve the issue?

A. CASB

B. AUP

C. NG-SWG

D. VPC endpoint

Correct Answer: A

QUESTION 2

Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

A. An SLA

B. An NDA

C. A BPA

D. An MOU

Correct Answer: A

Comptia exams are all about keywords and the catch here is "include monetary penalties for breaches". SLA includes penalties for not delivering services up to contract, BPA does not.

QUESTION 3

Development team members set up multiple application environments so they can develop, test, and deploy code in a secure and reliable manner. One of the environments is configured with real data that has been obfuscated so the team can adequately assess how the code will work in production. Which of the following environments is set up?

A. Quality assurance

B. Development

C. Sandbox

D. Production

Correct Answer: C

QUESTION 4

Which of the following provides guidelines for the management and reduction of information security risk?

A. CIS

B. NIST CSF

C. ISO

D. PCI DSS

Correct Answer: B

QUESTION 5

After a phishing scam for a user\\'s credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session

Which of the following types of attacks has occurred?

A. Privilege escalation

B. Session replay

C. Application programming interface

D. Directory traversal

Correct Answer: A

Privilege escalation DOES NOT always mean you are escalating to elevated permissions. Privilege escalations can also be horiztonal movements. In this case, the red team compromises a user\\'s account through the phising attack. The red team then deploys payload on the server through the comprised user account. The malware then initiates a new remote session, enabling the hackers to access the server directly. The comprised account is User A and the red team directly connected as a result of the malware can be thought of as User B. In this case, privilege escalation refers to user B being able to access user A resources.

QUESTION 6

Which of the follow ng disaster recovery sites is the most cost effective to operate?

A. Warm site

B. Cold site

C. Hot site

D. Hybrid site

Correct Answer: B

QUESTION 7

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow

B. Pass the hash

C. SQL injection

D. Replay attack

Correct Answer: B

QUESTION 8

A security analyst is tasked with classifying data to be stored on company servers. Which of the following should be classified as proprietary?

A. Customers\\' dates of birth

B. Customers\\' email addresses

C. Marketing strategies

D. Employee salaries

Correct Answer: C

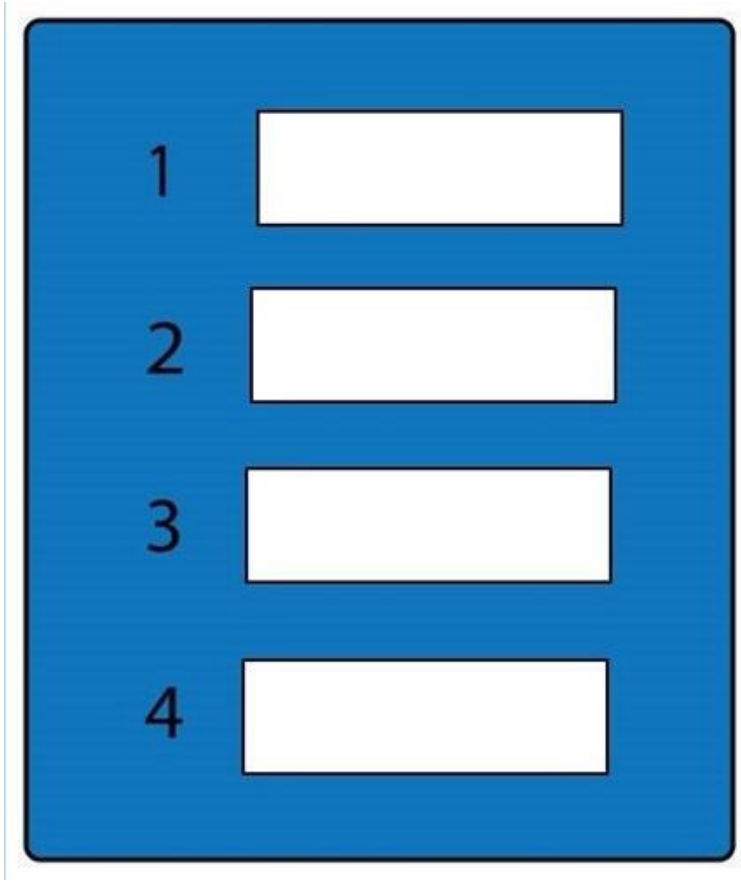
Proprietary Information" shall mean information (whether now existing or hereafter created or acquired) developed, created, or discovered by the Company, or which became known by, or was conveyed to the Company, which has commercial value in the Company\\'s business.

QUESTION 9

DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:



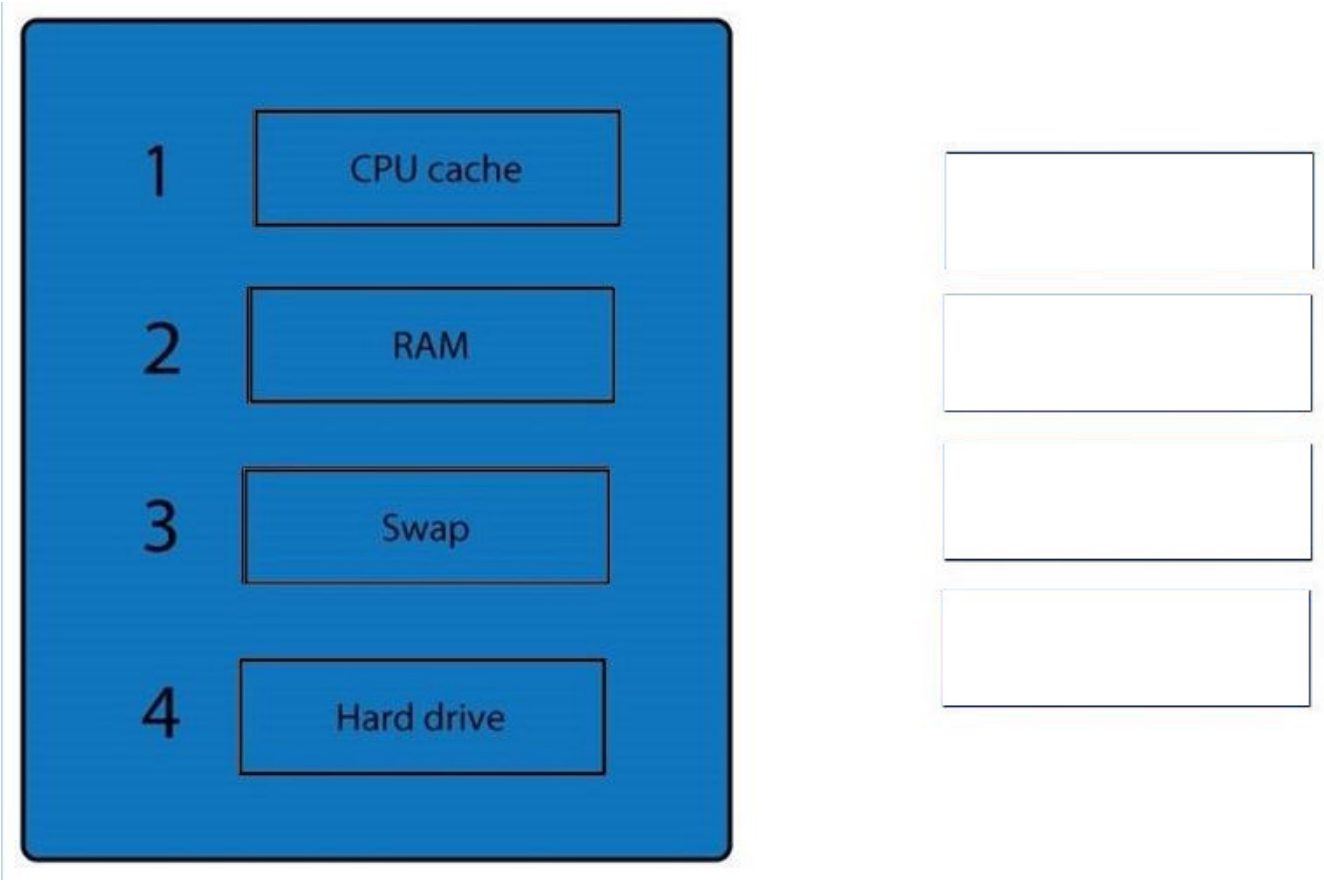
RAM

CPU cache

Swap

Hard drive

Correct Answer:



When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone.

Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and

printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and

expenses associated with the investigation.

QUESTION 10

After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company Which of the following risk management strategies is the manager adopting?

A. Risk acceptance

B. Risk avoidance

C. Risk transference

D. Risk mitigation

Correct Answer: C

whenever risk management is outsourced the risk is said to be transfered

---

QUESTION 11

A security analyst is reviewing a secure website that is generating TLS certificate errors. The analyst determines that the browser is unable to receive a response from the OCSP for the certificate. Which of the following actions would most likely resolve the issue?

A. Run a traceroute on the OCSP domain to find where the domain is failing.

B. Create an exclusion for the OCSP domain in the content filter

C. Unblock the OCSP protocol in the host-based firewall

D. Add the root certificate to the trusted sites on the workstation with the issue.

Correct Answer: C

QUESTION 12

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer

B. The data processor

C. The data owner

D. The data controller

Correct Answer: D

Data Owner and Data Controller are very similar concepts, but Data Controller is a GDPR term, and Data Owner isn\\'t. The question specifically asks for a GDPR term.