SY0-601Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.leads4pass.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

A security operations technician is searching the log named /vax/messages for any events that were associated with a workstation with the IP address 10.1.1.1.

Which of the following would provide this information?

A. cat /var/messages | grep 10.1.1.1

B. grep 10.1.1.1 | cat /var/messages

C. grep /var/messages | cat 10.1.1.1

D. cat 10.1.1.1 | grep /var/messages

Correct Answer: A

the cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex. The cut command splits each line into fields based on a delimiter and extracts a specific field.

QUESTION 2

A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identify the weak spots.

B. Use a packet analyzer to investigate the NetFlow traffic

C. Check the SIEM to review the correlated logs.

D. Require access to the routers to view current sessions,

Correct Answer: C

A SIEM (Security Information and Event Management) system collects and aggregates logs from various sources across an enterprise\\'s network and IT infrastructure. It can correlate and analyze these logs to identify security incidents and provide a comprehensive view of activities across the network. In the case of a data breach investigation, the SIEM can be a valuable tool to review the logs generated during the attack and trace the attacker\\'s activities from the perimeter network to the sensitive information.

QUESTION 3

Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

A. Mantraps

B. Security guards

C. Video surveillance

D. Fences

E. Bollards

F. Antivirus

Correct Answer: AB

A - a mantrap can trap those personnal with bad intension(preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnal from approaching as well(deterrent) B security guards can sure do the same thing as above, preventing malicious personnal from entering(preventive+deterrent), and notice those personnal as well(detective)

QUESTION 4

Ann. a forensic analyst. needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?

A. Chain of custody

B. Checksums

C. Non-repudiaton

D. Legal hold

Correct Answer: B

If the checksum of the original file is known, an authorized user can run a checksum/hashing utility on the file to match the resulting checksum to the original checksum. If these two checksums match, the file is identical. However, if they don\\'t match, the user can identify a fake version of the original file.

Checksums are used to check files and other data for errors or manipulation that might have occurred during data transmission or storage.

QUESTION 5

An employee\\'s company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

A. a push notification

B. a password

C. an SMS message

D. an authentication application

Correct Answer: A

SY0-601 PDF Dumps SY0-601 Practice Test SY0-601 Braindumps