GSEC Q&As

GIAC Security Essentials Certification

Pass GIAC GSEC Exam with 100% Guarantee

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

https://www.geekcert.com/gsec.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

What method do Unix-type systems use to prevent attackers from cracking passwords using pre-computed hashes?

A. Unix systems can prevent users from using dictionary words for passwords

B. The algorithms creates hashes using a CPU- intensive algorithm.

C. The algorithm creates hashes using salts or randomized values

D. Unix/Linux systems use hashing functions which cannot be reversed

E. The system encrypts the password using a symmetrical algorithm

Correct Answer: C

QUESTION 2

Which of the following is an advantage of private circuits versus VPNs?

A. Flexibility

B. Performance guarantees

C. Cost

D. Time required to implement

Correct Answer: B

QUESTION 3

Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?

A. Analysis of encrypted traffic

B. Provide insight into network traffic

C. Detection of network operations problems

D. Provide logs of network traffic that can be used as part of other security measures.

E. Inexpensive to manage

F. B, C, and D

G. A, C, and E

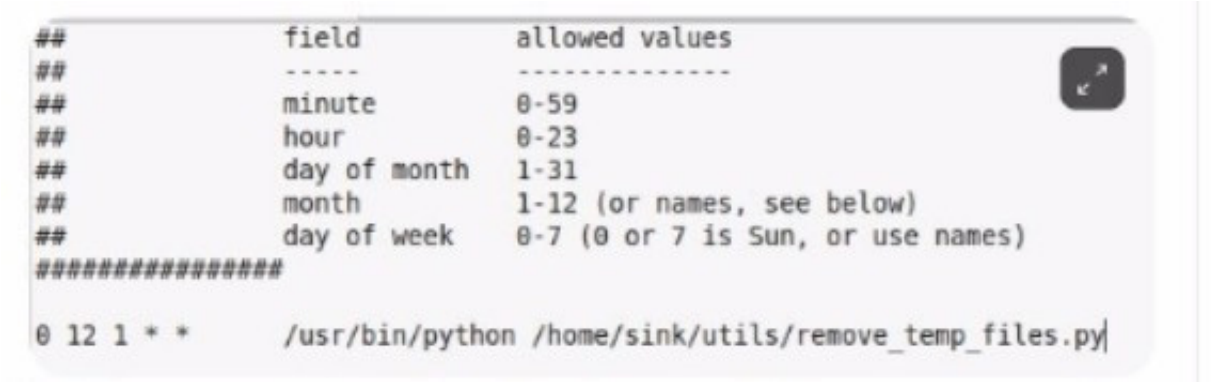
H. B, D, and E

I. A, B, and C

Correct Answer: C

QUESTION 4

Analyze the file below. When will the program /home/sink/utils/remove temp hies.py run?



A. When a user requests it by connecting to the listening port

B. When the user \\'sink\\' logs in

C. At startup when the system enters the multi-user runlevel

D. At the time specified in the crontab file

Correct Answer: D

QUESTION 5

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag.

B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody.

C. Take photographs of all persons who have had access to the computer.

D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag.

Correct Answer: D