SY0-401 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-401 Exam with 100% Guarantee

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

https://www.geekcert.com/SY0-401.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

QUESTION 1

Security administrator receives reports from various organizations that a system on the company network is port scanning hosts on various networks across the internet. The administrator determines that the compromised system is a Linux host and notifies the owner that the system will be quarantined and isolated from the network. The system does not contain confidential data, and the root user was not compromised. The administrator would like to know how the system was compromised, what the attackers did, and what remnants he attackers may have left behind. Which of the following are the administrator\\'s NEXT steps in the investigation? (Select Two)

A. Reinstall the procps package in case system utilities were modified

B. Look for recent modified files in user and tmp directions

C. Switch SELinux to enforcing mode and reboot

D. Monitor perimeter firewall for suspicious traffic from the system

E. Check running processes and kernel modules

F. Remove unnecessary accounts and services

Correct Answer: CD

QUESTION 2

During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping

B. Vulnerability scan

C. Port Scan

D. Protocol analysis

Correct Answer: B

QUESTION 3

Which of the following is an attack designed to activate based on time?

A. Logic Bomb

B. Backdoor

C. Trojan

D. Rootkit

Correct Answer: A

QUESTION 4

A recent audit has revealed that several users have retained permissions to systems they should no longer have rights to after being promoted or changed job positions. Which of the following controls would BEST mitigate this issue?

A. Separation of duties

B. User account reviews

C. Group based privileges

D. Acceptable use policies

Correct Answer: A

QUESTION 5

Which of the following is the default port for TFTP?

A. 20

B. 69

C. 21

D. 68

Correct Answer: B

TFTP makes use of UDP port 69.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.geekcert.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: