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

A company is rolling out a new e-commerce website. The security analyst wants to reduce the risk of the new website being comprised by confirming that system patches are up to date, application hot fixes are current, and unneeded ports and services have been disabled. To do this, the security analyst will perform a:

A. Vulnerability assessment

B. White box test

C. Penetration test

D. Peer review

Correct Answer: A

QUESTION 2

Ann the IT director wants to ensure that as hoc changes are not making their way to the production applications. Which of the following risk mitigation strategies should she implement in her department?

A. Change management

B. Permission reviews

C. Incident management

D. Perform routine audits

Correct Answer: A

QUESTION 3

Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

A. Virtualization

B. Remote access

C. Network access control

D. Blade servers

Correct Answer: A

Because Virtualization allows a single set of hardware to host multiple virtual machines, it requires less hardware to maintain the current scenario.

QUESTION 4

Joe the system administrator has noticed an increase in network activity from outside sources. He wishes to direct traffic to avoid possible penetration while heavily monitoring the traffic with little to no impact on the current server load. Which of the following would be BEST course of action?

A. Apply an additional firewall ruleset on the user PCs.

B. Configure several servers into a honeynet

C. Implement an IDS to protect against intrusion

D. Enable DNS logging to capture abnormal traffic

Correct Answer: B

QUESTION 5

In the course of troubleshooting wireless issues from users a technician discovers that users are connecting to their home SSIDs which the technician scans but detects none of these SSIDs. The technician eventually discovers a rouge access point that spoofs any SSID request. Which of the following allows wireless use while mitigating this type of attack?

A. Configure the device to verify access point MAC addresses

B. Disable automatic connection to known SSIDs

C. Only connect to trusted wireless networks

D. Enable MAC filtering on the wireless access point

Correct Answer: A

Latest SY0-401 Dumps SY0-401 VCE Dumps SY0-401 Exam Questions

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

Try our product !

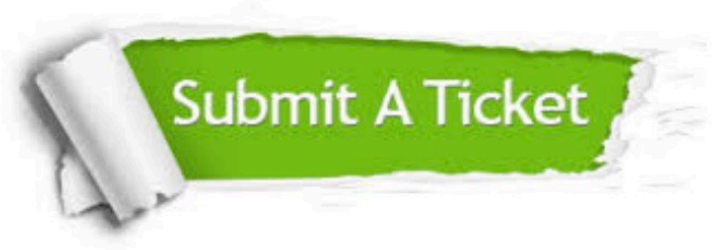
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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:



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © geekcert, All Rights Reserved.