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.passapply.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 security administrator is reviewing logs and notices multiple attempts to access the HVAC controls by a workstation with an IP address from the open wireless network. Which of the following would be the best way to prevent this type of attack from occurring again?

A. Implement VLANs to separate the HVAC

B. Enable WPA2 security for the wireless network

C. Install a HIDS to protect the HVAC system

D. Enable Mac filtering for the wireless network

Correct Answer: D

QUESTION 2

A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

A. Bind server

B. Apache server

C. Exchange server

D. RADIUS server

Correct Answer: A

BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. It includes the DNS server component contracted for name daemon. This is the only option that directly involves DNS.

QUESTION 3

Joe, a security analyst, is attempting to determine if a new server meets the security requirements of his organization. As a step in this process, he attempts to identify a lack of security controls and to identify common misconfigurations on the server. Which of the following is Joe attempting to complete?

A. Black hat testing

B. Vulnerability scanning

C. Black box testing

D. Penetration testing

Correct Answer: B

QUESTION 4

A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database. Which of the following risk mitigation startegies should have been implemented when the supervisor was demoted?

A. Incident management

B. Routine auditing

C. IT governance

D. Monthly user rights reviews

Correct Answer: D

QUESTION 5

After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely. Which of the following is the MOST likely reason the PC technician is unable to ping those devices?

A. ICMP is being blocked

B. SSH is not enabled

C. DNS settings are wrong

D. SNMP is not configured properly

Correct Answer: A

ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping. ICMP offers no information If ICMP request queries go unanswered, or ICMP replies are lost or blocked.

[Latest SY0-401 Dumps](#)   [SY0-401 VCE Dumps](#)   [SY0-401 Braindumps](#)

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
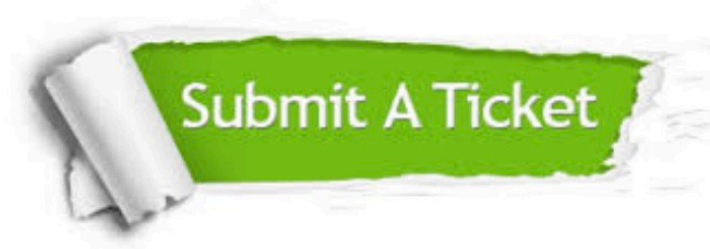Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.passapply.com/allproducts

Need Help

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