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

Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

A. Single sign on

B. IPv6

C. Secure zone transfers

D. VoIP

Correct Answer: C

C: A primary DNS server has the "master copy" of a zone, and secondary DNS servers keep copies of the zone for redundancy. When changes are made to zone data on the primary DNS server, these changes must be distributed to the secondary DNS servers for the zone. This is done through zone transfers. If you allow zone transfers to any server, all the resource records in the zone are viewable by any host that can contact your DNS server. Thus you will need to secure the zone transfers to stop an attacker from mapping out your addresses and devices on your network.

QUESTION 2

A security administrator wishes to prevent certain company devices from using specific access points, while still allowing them on others. All of the access points use the same SSID and wireless password. Which of the following would be MOST appropriate in this scenario?

A. Require clients to use 802.1x with EAPOL in order to restrict access

B. Implement a MAC filter on the desired access points

C. Upgrade the access points to WPA2 encryption

D. Use low range antennas on the access points that ne4ed to be restricted

Correct Answer: B

QUESTION 3

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5

B. WEP

C. PEAP-MSCHAPv2

D. EAP-TLS

Correct Answer: C

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

QUESTION 4

An administrator is hardening systems and wants to disable unnecessary services. One Linux server hosts files used by a Windows web server on another machine. The Linux server is only used for secure file transfer, but requires a share for the Windows web server as well. The administrator sees the following output from a netstat -1p command:

```
Proto Recv-Q      Send-Q        Local Addr Foreign Addr      State PID
tcp    0    0     *:mysql      *;*   LISTEN      1488/mysqld
tcp    0    0     *:ftp *;*    LISTEN      2120/vsftpd
tcp    0    0     *:80  *;*    LISTEN      1680/httpd
udp    0    0     *:69  *;*    LISTEN      2680/tftp
tcp    0    0     *:139 *;*    LISTEN      8217/smbd
tcp    0    0     *:6667     *;*   LISTEN      2121/badBunny_FTP
```

Which of the following processes can the administrator kill without risking impact to the purpose and function of the Linux or Windows servers? (Select Three)

A. 1488

B. 1680

C. 2120

D. 2121

E. 2680

F. 8217

Correct Answer: ADF

QUESTION 5

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access

B. Spoofing

C. Man-in-the-middle

D. Replay

Correct Answer: C

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: