SY0-501^{Q&As}

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.passapply.com/sy0-501.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 developer is creating a new web application on a public cloud platform and wants to ensure the application can respond to increase in load while minimizing costs during periods of low usage. Which of the following strategies is MOST relevant to the use-case?

A. Elasticity

B. Redundancy

C. High availability

D. Non-persistence

Correct Answer: A

QUESTION 2

Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.

B. The recipient can verify the authenticity of the site used to download the patch.

C. The recipient can request future updates to the software using the published MD5 value.

D. The recipient can successfully activate the new software patch.

Correct Answer: A

QUESTION 3

Which of the following is an asymmetric function that generates a new and separate key every time it runs?

A. RSA

B. DSA

C. DHE

D. HMAC

E. PBKDF2

Correct Answer: C

QUESTION 4

Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company\\'s final software releases? (Select TWO)

A. Unsecure protocols

B. Use of penetration-testing utilities

C. Weak passwords

D. included third-party libraries

E. Vendors/supply chain

F. Outdated anti-malware software

Correct Answer: AC

QUESTION 5

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING:   REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks Is the researcher MOST likely experiencing?

A. MAC cloning

B. Evil twin

C. Man-in-the-middle

D. ARP poisoning

Correct Answer: C

This is alarming because it could actually mean that you\\'re connecting to a different server without knowing it. If this new server is malicious then it would be able to view all data sent to and from your connection, which could be used by whoever set up the server. This is called a man-in-the-middle attack. This scenario is exactly what the "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!" message is trying to warn you about.