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.pass4itsure.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

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its dat

A. In which of the following documents would this concern MOST likely be addressed?

B. Service level agreement

C. Interconnection security agreement

D. Non-disclosure agreement

E. Business process analysis

Correct Answer: A

QUESTION 2

A company notices that at 10 a.m. every Thursday, three users\\' computers become inoperable. The security analyst team discovers a file called where.pdf.exe that runs on system startup. The contents of where.pdf.exe are shown below:

@echo off if [c:\file.txt] deltree C:\

Based on the above information, which of the following types of malware was discovered?

A. Rootkit

B. Backdoor

C. Logic bomb

D. RAT

Correct Answer: C

QUESTION 3

Which of the following are considered to be "something you do"? (Select TWO).

A. Iris scan

B. Handwriting

C. Common Access Card

D. Gait

E. PIN

F. Fingerprint

Correct Answer: BD

QUESTION 4

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

A. Password complexity rules

B. Continuous monitoring

C. User access reviews

D. Account lockout policies

Correct Answer: B

QUESTION 5

Which of the following is a major difference between XSS attacks and remote code exploits?

A. XSS attacks use machine language, while remote exploits use interpreted language

B. XSS attacks target servers, while remote code exploits target clients

C. Remote code exploits aim to escalate attackers\\' privileges, while XSS attacks aim to gain access only

D. Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

Correct Answer: A