EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **SY0-501**

Title : CompTIA Security+

Version : DEMO

1. Topic 1, Exam Pool A

A security analyst received an after-hours alert indicating that a large number of accounts with the suffix "admin'' were locked out. The accounts were all locked out after five unsuccessful login attempts, and no other accounts on the network triggered the same alert.
Which of the following is the BEST explanation for these alerts?
A. The standard naming convention makes administrator accounts easy to identify, and they were targeted for an attack.
B. The administrator accounts do not have rigid password complexity rules, and this made them easier to crack.
C. The company has implemented time-of-day restrictions, and this triggered a false positive alert when the administrators tried to log in
D. The threshold for locking out administrator accounts is too high, and it should be changed from five to three to prevent unauthorized access attempts.
Answer: A

2.A systems administrator is increasing the security settings on a virtual host to ensure users on one VM cannot access information from another VM.
Which of the following is the administrator protecting against?
A. VM sprawl
B. VM escape
C. VM migration
D. VM sandboxing
Answer: B

3.A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers.
A systems administrator is concerned about the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?
A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters
Answer: A

4.A credentialed vulnerability scan is often preferred over a non-credentialed scan because credentialed scans:
A. generates more false positives.
B. rely solely on passive measures.
C. are always non-intrusive.
D. provide more accurate data.
Answer: C

5.Fuzzing is used to reveal which of the following vulnerabilities in web applications?
A. Weak cipher suites
B. Improper input handling
C. DLL injection
D. Certificate signing flaws
Answer: B