SY0-601$^{\text{Q\&As}}$

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

QUESTION 1

A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?

A. SSO

B. IDS

C. MFA

D. TPM

Correct Answer: C

MFA = harder to impersonate due to having multifactor authentication.

QUESTION 2

A company would like to move to the cloud. The company wants to prioritize control and security over cost and ease of management. Which of the following cloud models would best suit this company\\'s priorities?

A. Public

B. Hybrid

C. Community

D. Private

Correct Answer: D

A private cloud model would best suit the company\\'s priorities of control and security over cost and ease of management. In a private cloud, the infrastructure is dedicated to a single organization, providing greater control over the environment and the ability to implement strict security measures. This is in contrast to public, community, or hybrid cloud models, where resources are shared among multiple organizations, potentially compromising control and security. While private clouds can be more expensive and more difficult to manage, they the highest level of control and security for the company.

Reference:

-

CompTIA Security+ Certification Exam Objectives (SY0-601), Section 3.2: "Explain the importance of secure staging deployment concepts."

-

Cisco: Private Cloud - https://www.cisco.com/c/en/us/solutions/cloud/private-cloud.html

QUESTION 3

A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are being transmitted and stored more securely?

A. Blockchain

B. Salting

C. Quantum

D. Digital signature

Correct Answer: B

Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the

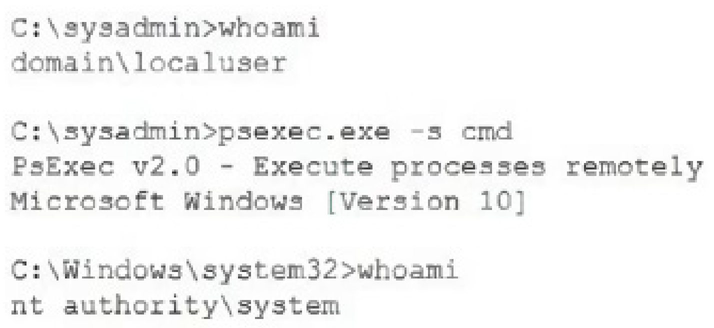
same password will have different hashed credentials.

A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them

harder to crack or reverse.

QUESTION 4

A security analyst is reviewing the following system command history on a computer that was recently utilized in a larger attack on the corporate infrastructure:



```
C:\sysadmin>whoami
domain\localuser

C:\sysadmin>psexec.exe -s cmd
PsExec v2.0 - Execute processes remotely
Microsoft Windows [Version 10]

C:\Windows\system32>whoami
nt authority\system
```

Which of the following best describes what the analyst has discovered?

A. A successful privilege escalation attack by a local user

B. A user determining what level of permissions the user has

C. A systems administrator performing routine maintenance

D. An attempt to utilize living-off-the-land binaries

Correct Answer: A

QUESTION 5

An enterpnse has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box

B. Red-leam

C. Bug bounty

D. Gray-box

E. Black-box

Correct Answer: C

A bug bounty program provides a monetary incentive for security researchers to discover vulnerabilities. One of the benefits is that bug bounty programs only pay researchers when they find vulnerabilities. Companies don\\'t pay researchers for their time.

Reference: https://en.wikipedia.org/wiki/Bug_bounty_program