07: Lab 07: Managing Password Security

Security+ (Exam SY0-701)

10/10

Congratulations, you passed!

Duration: 28 minutes, 11 seconds

☑ **Confirm pass.txt contents**   *Score: 1*

Select the **Score** button to validate this task:
File /root/pass.txt exists and contains 'Pa$$w0rd'
Task complete

☑ Which two accounts are using the same password?   *Score: 1*

- ☑ Jaime
- ☑ Admin
- ☐ Alex
- ☐ Jordan
- ☐ Logan

Congratulations, you have answered the question correctly.

☑ **confirm the existence of /root/dict-cracked.txt**   *Score: 1*

Select the **Score** button to validate this task:
File /root/dict-cracked.txt exists and contains '123456'
Task complete

☑ **confirm the existence of /root/brute-cracked.txt**   *Score: 1*

Select the **Score** button to validate this task:
File /root/brute-cracked.txt exists and contains '123456'
Task complete

☑ What domain password policy settings are currently defined? (Select all that apply) *Score: 1*

- ☑ ComplexityEnabled: True
- ☐ LockoutDuration: 00:15:00
- ☑ LockoutThreshold: 0
- ☑ MaxPasswordAge: 42
- ☐ MinPasswordAge: 3
- ☑ MinPasswordLength: 7

Congratulations, you have answered the question correctly.

☑ What is password spraying?   *Score: 1*

    ◉ <u>Trying a known password against many user accounts</u>
    ○ Guessing a password for a user account
    ○ Extracting password hashes for user accounts
    ○ Trying numerous combinations of characters to discover a password

Congratulations, you have answered the question correctly.

☑ What security measure is a password spraying attack attempting to avoid or bypass?   *Score: 1*

    ◉ <u>Account lockout</u>
    ○ Maximum password age
    ○ Minimum password length
    ○ Complexity requirements

Congratulations, you have answered the question correctly.

☑ What is the primary factor that determines the likelihood of success of dictionary password cracking?   *Score: 1*

    ◉ <u>size of the dictionary file</u>
    ○ length of the password
    ○ complexity of the password
    ○ age of the password
    ○ account lockout

Congratulations, you have answered the question correctly.

☑ What aspects of a target's password are a defense against brute force password cracking? (Select all that apply)   *Score: 1*

    ☐ greater age
    ☑ <u>longer length</u>
    ☐ ease to pronounce
    ☑ <u>increased complexity</u>
    ☐ using well-known algorithms

Congratulations, you have answered the question correctly.

☑ Which domain password policy settings has the greatest impact on strength (i.e., resistance to brute force attacks)?   *Score: 1*

    ◉ <u>MinPasswordLength</u>
    ○ ComplexityEnabled
    ○ MaxPasswordAge
    ○ PasswordHistoryCount

Congratulations, you have answered the question correctly.