Exam Report: 7.2.5 Practice Questions

Date: 1/22/2020 1:55:48 pm
Time Spent: 2:47

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

In a variation of the brute force attack, an attacker may use a predefined list (dictionary) of common user names and passwords to gain access to existing user accounts. Which countermeasure best addresses this issue?

- A strong password policy
- VLANs
- 3DES encryption
- AES encryption

Explanation

A strong password policy is the best defense against dictionary attacks. The policy must be enforced, and all users must be trained to properly construct and protect strong passwords.

3DES and AES encryption alone do not protect against dictionary attacks. Encryption technologies are useless if weak passwords permit easy access to encrypted channels.

VLANs allow logical segmentation of a physical network and do not prevent dictionary attacks and weak passwords.

References

LabSim for Security Pro, Section 7.2.
[All Questions SecPro2017_v6.exm PASSWORD_ATTACKS_01]

Question 2: Correct

Which of the following password attacks uses preconfigured matrices of hashed dictionary words?

- Dictionary
- Rainbow table
- Hybrid
- Brute force

Explanation

A *rainbow table* attack applies hashing algorithms to every word in a dictionary (sometimes including hybrids or passwords accumulated in brute force techniques). It then saves the results in a table or matrix. An encrypted password is compared to the pre-computed hashed passwords in the matrix until a match is found.

A *dictionary* attack tries known words (such as from a dictionary). A *brute force* attack works through all possibilities until the password is cracked. A *hybrid* attack adds appendages to known dictionary words (for example, 1password, password07, and p@ssword1).

References

LabSim for Security Pro, Section 7.2.
[All Questions SecPro2017_v6.exm PASSWORD_ATTACKS_02]

Question 3: Correct

Which of the following is most vulnerable to a brute force attack?

- Biometric authentication
- Challenge-response token authentication
- Two-factor authentication
- Password authentication

Explanation

Password authentication is the most vulnerable to a brute force attack. The brute force attack itself may take a considerable amount of time, especially if the attack is against a single user account or online login prompt rather than a localized copy of a security accounts database. However, once the attack is complete, the attacker has all they need to log in to the secured system.

References

LabSim for Security Pro, Section 7.2.
[All Questions SecPro2017_v6.exm PASSWORD_ATTACKS_03]

Question 4: Correct

A user named Bob Smith has been assigned a new desktop workstation to complete his day-to-day work.

When provisioning Bob's user account in your organization's domain, you assigned an account name of **BSmith** with an initial password of **bw2Fs3d**.

On first login, Bob is prompted to change his password, so he changes it to the name of his dog (**Fido**).

What should you do to increase the security of Bob's account? (Select two.)

- [ ] Use a stronger initial password when creating user accounts.
- [ ] Configure user account names that are not easy to guess.
- [ ] Require him to use the initial password, which meets the complexity requirements.
- [x] Train users not to use passwords that are easy to guess.
- [ ] Do no allow users to change their own passwords.
- [x] Use Group Policy to require strong passwords on user accounts.

Explanation

In this scenario, a weak password that is easy to guess has been used. To prevent this type of password, you should:

- Use Group Policy to require strong passwords on user accounts. In this example, **Fido** is a weak password because it is short and doesn't contain numbers or other non-alphabetic characters.
- Train users not to use passwords that are easy to guess. In this example, the user's password could very likely be guessed using basic reconnaissance techniques on social media websites.

You should allow users to set their own passwords. If you don't, then both the administrator and the user know the password, which is a poor security practice. Using a stronger initial password will not prevent the user from using a weak password if the appropriate Group Policy settings aren't in force. Creating user account names such as the one shown in this scenario is generally considered an acceptable security practice. Requiring users to use assigned passwords, even if they are complex, is not secure because passwords should not be known by anyone but the user.

References

LabSim for Security Pro, Section 7.2.
[All Questions SecPro2017_v6.exm PASSWORD_ATTACKS_04]

Question 5: Incorrect

Which of the following strategies can protect against a rainbow table password attack?

- ~~Encrypt the password file with one-way encryption~~
- Enforce strict password restrictions
- Educate users to resist social engineering attacks
- Add random bits to the password before hashing takes place

Explanation

Some authentication protocols send password hashes instead of the actual password between systems during the authentication process. Rainbow table attacks apply hashing algorithms to every word in a dictionary (sometimes including hybrids or passwords accumulated in brute force techniques) in an attempt to match hashed passwords. To protect against this type of attack, you can salt the hash by adding random bits to the password before hashing takes place, thereby producing an entirely different hash value for the password. Because the hacker does not know the extra random bits, the rainbow table will be of no value.

The password file should be encrypted, but rainbow attacks do not work by accessing the password, file but by capturing hashed passwords being transmitted on the network. Users should be educated about social engineering attacks, but there is no connection between social engineering and rainbow table attacks. Enforcing strict password restrictions might actually weaken network security if you do not educate users about proper procedures to take to protect login credentials.

References

LabSim for Security Pro, Section 7.2.
[All Questions SecPro2017_v6.exm PASSWORD_ATTACKS_05]