Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/13/2022 8:13:48 pm • Time spent: 02:14

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

You are using a password attack that tests every possible keystroke for each single key in a password until the correct one is found. Which of the following technical password attacks are you using?

- Keylogger
- Password sniffing
- Brute force attack
- Pass-the-hash attack

EXPLANATION

In a brute force attack, every password is eventually found because the technique is to test every possible keystroke for each single key in a password until the correct one is found.

Keyloggers log or record every keystroke on the computer keyboard to obtain passwords and other important data.

A pass-the-hash attack is a hacking technique where an attacker uses an underlying NTLM or hash of a user's password to gain access to a server without ever using the actual plaintext password.

Password sniffing is a passive way for attackers to gain access to an account. The sniffer collects data that is in transit in a LAN. If access is gained on one system in a LAN, data can be gathered from data being sent from any other system in the network. The sniffer runs in the background, making it undetectable.

REFERENCES

11.7.2 Password Attack Facts

q_pwd_attacks_brute_02_secp7.question.fex

Question 2: ✔ 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. 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.
- [ ] Require him to use the initial password, which meets the complexity requirements.
- [ ] Configure user account names that are not easy to guess.
- [ ] Do not allow users to change their own passwords.
- [x] Use Group Policy to require strong passwords on user accounts.
- [x] Train users not to use passwords that are easy to guess.

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, both the administrator and the user know the password, which is a poor security practice. Using a stronger initial password does 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

11.7.2 Password Attack Facts

q_pwd_attacks_complex_secp7.question.fex

Question 3: ✔ Correct

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

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

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 or weak passwords.

REFERENCES

11.7.2 Password Attack Facts

q_pwd_attacks_dictionary_secp7.question.fex

Question 4: ✔ Correct

You are cleaning your desk at work. You toss several stacks of paper in the trash, including a sticky note with your password written on it. Which of the following types of non-technical password attacks have you enabled?

- Social engineering
- Shoulder surfing
- Password guessing
- Dumpster diving

EXPLANATION

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Social engineering relies on human error. It works by feigning trustworthiness to convince someone to give the attacker access.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like a pet's name or a hobby.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 11.7.2 Password Attack Facts

q_pwd_attacks_dumpster_secp7.question.fex

Question 5: ✔ Correct

Carl received a phone call from a woman who states that she is calling from his bank. She tells him that someone has tried to access his checking account, and she needs him to confirm his account number and password to discuss further details. He gives her his account number and password. Which of the following types of non-technical password attack has occurred?

- Password guessing
- Social engineering
- Dumpster diving
- Shoulder surfing

EXPLANATION

Social engineering relies on human error. It works by feigning trustworthiness to convince someone to share information.

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like a pet's name or a hobby.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 11.7.2 Password Attack Facts

q_pwd_attacks_imperson_secp7.question.fex

Question 6: ✔ Correct

You want to check a server for user accounts that have weak passwords. Which tool should you use?

- Nessus
- OVAL
- Retina
- John the Ripper

EXPLANATION

John the Ripper is a password cracking tool. Password crackers perform cryptographic attacks on passwords. Use a password cracker to identify weak passwords or passwords protected with weak encryption.

Nessus and Retina are vulnerability scanners. While vulnerability scanners check for default user accounts and often check for accounts with blank passwords, they typically do not include password cracking features to test for weak passwords.

The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

REFERENCES

5.9.2 Device Vulnerability Facts

11.7.2 Password Attack Facts

11.7.5 Crack Passwords

11.7.6 Crack Password Protected Files

11.7.7 Crack a Password with John the Ripper

q_pwd_attacks_pass_crack_secp7.question.fex

Question 7: ✔ Correct

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

- Hybrid attack
- Dictionary attack
- Rainbow table attack
- Brute-force attack

EXPLANATION

A rainbow table attack applies hashing algorithms to every word in a dictionary (sometimes including hybrids or passwords accumulated in brute force techniques). The algorithm 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

11.7.2 Password Attack Facts

q_pwd_attacks_rainbow_01_secp7.question.fex

Question 8: ✔ Correct

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

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

EXPLANATION

Some authentication protocols send password hashes 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 is 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 that protect login credentials.

REFERENCES

11.7.2 Password Attack Facts

q_pwd_attacks_rainbow_02_secp7.question.fex

Question 9: ✔ Correct

Which of the following techniques involves adding random bits of data to a password before it is stored as a hash?

- Password sniffing
- Keylogging
- Password salting
- Pass-the-hash attack

EXPLANATION

Password salting is adding random bits of data to a password before it is stored as a hash, making password cracking much more difficult.

Password sniffing is a passive way for attackers to gain access to an account. The sniffer collects data that is in transit in a LAN.

A pass-the-hash attack is a hacking technique where an attacker uses an underlying NTML or hash of a user's password to gain access to a server without ever using the actual plaintext password.

Keylogging is recording every stroke on the computer keyboard.

REFERENCES

7.3.3 Hashing Facts

11.7.2 Password Attack Facts

q_pwd_attacks_salting_secp7.question.fex

Question 10: ✔ Correct

Which of the following best describes shoulder surfing?

- Finding someone's password in the trash can and using it to access their account.
- Guessing someone's password because it is so common or simple.
- ➡ Someone nearby watching you enter your password on your computer and recording it.
- Giving someone you trust your username and account password.

EXPLANATION

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like their pet's name or their hobby.

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Social engineering relies on human error. It works by convincing someone to give the attacker access because he or she tricks them into trusting him or her.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 11.7.2 Password Attack Facts

q_pwd_attacks_shoulder_secp7.question.fex