Exam Report: 15.4.4 Practice Questions

Date: 5/26/2020 7:43:46 pm
Time Spent: 0:39

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following best explains why brute force attacks are always successful?

- They test every possible valid combination.
- They are fast.
- ~~They can be performed in a distributed parallel processing environment.~~
- They are platform-independent.

Explanation

Brute force attacks are always successful because they test every possible valid combination. Therefore, they will eventually discover the actual key, password, or code that was used.

Brute force attacks are not fast.

Brute force attacks are platform-independent, but this fact does not affect their level of success.

Brute force attacks can be deployed in distributed parallel processing environments in order to make them faster, but this is not necessary make them successful.

References

TestOut Ethical Hacker Pro - 15.4 Cryptanalysis and Cryptographic Attack Countermeasures
[e_cryptanalysis_eh1.exam.xml Q_CRYPTANALYSIS_BREAK_METHODS_01_EH1]

Question 2: Incorrect

Which of the following cryptography attacks is characterized by the attacker having access to both the plain text and the resulting ciphertext, but does not allow the attacker to choose the plain text?

- Chosen ciphertext
- Chosen plain text
- ~~Brute force~~
- Known plain text

Explanation

A known plain text attack is characterized by the attacker having access to both the plain text and the resulting ciphertext. The attacker can make conclusions about the encrypting key and will have validation if the encrypting key is discovered.

A chosen plain text attack is characterized by the attacker choosing the plain text to be encrypted. The main difference between known plain text and chosen plain text is the attacker's ability to select random plain text and run it through the encrypting mechanism.

A brute force attack is characterized by the attacker trying every known combination.

A chosen ciphertext attack is characterized by the attacker producing ciphertext and then sending it through a decryption process to see the resulting plain text.

References

TestOut Ethical Hacker Pro - 15.4 Cryptanalysis and Cryptographic Attack Countermeasures
[e_cryptanalysis_eh1.exam.xml Q_CRYPTANALYSIS_CRY_ATTACKS_01_EH1]

Question 3: Correct

Your company produces an encryption device that lets you enter text and receive encrypted text in response. An attacker obtains one of these devices and starts inputting random plain text to see the resulting ciphertext. Which of the following cryptographic attacks is being used?

- (selected) Chosen plain text
- Chosen ciphertext
- Known plain text
- Brute force

Explanation

A chosen plain text attack is when the attacker chooses the plaintext to be encrypted. The attacker can choose the plain text that will produce clues to the encryption key used.

A brute force attack is when the attacker tries every known combination.

A chosen ciphertext attack is when the attacker produces ciphertext and then sends it through a decryption process to see the resulting plain text.

A known plain text attack is when an attacker has seen the plain text and the resulting ciphertext, but is not able to choose the plain text to be encrypted.

References

TestOut Ethical Hacker Pro - 15.4 Cryptanalysis and Cryptographic Attack Countermeasures
[e_cryptanalysis_eh1.exam.xml Q_CRYPTANALYSIS_CRY_ATTACKS_02_EH1]

Question 4: Correct

Which of the following cryptography attacks is characterized by the attacker making a series of interactive queries and choosing subsequent plain texts based on the information from the previous encryption?

- Chosen ciphertext
- Chosen plain text
- Known plain text
- (selected) Adaptive chosen plain text

Explanation

An adaptive chosen plain text attack is characterized by the attacker making a series of interactive queries and choosing subsequent plain texts based on the information from the previous encryptions.

A known plain text attack is characterized by the attacker having access to both the plain text and the resulting ciphertext. The attacker can make conclusions about the encrypting key and will have validation if the encrypting key is discovered.

A chosen plain text attack is characterized by the attacker choosing the plain text to be encrypted. The main difference between known plain text and chosen plain text is the attacker's ability to select random plain text and run it through the encrypting mechanism.

A chosen ciphertext attack is characterized by the attacker producing ciphertext and then sending it through a decryption process to see the resulting plain text.

References

TestOut Ethical Hacker Pro - 15.4 Cryptanalysis and Cryptographic Attack Countermeasures

[e_cryptanalysis_eh1.exam.xml Q_CRYPTANALYSIS_CRY_ATTACKS_03_EH1]

Question 5: Incorrect

Which type of cryptanalysis method is based on substitution-permutation networks?

- Linear
- Dictionary
- ~~Differential~~
- Integral

Explanation

Integral cryptanalysis is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis.

Linear cryptanalysis is based on finding affine approximations to the action of a cipher. It is commonly used on block ciphers and works based on statistical differences between plaintext and ciphertext.

Differential cryptanalysis is a form of cryptanalysis applicable to symmetric key algorithms and works on statistical differences between ciphertexts of chosen data.

A dictionary attack is a type of cryptographic attack, not a cryptanalysis method.

References

TestOut Ethical Hacker Pro - 15.4 Cryptanalysis and Cryptographic Attack Countermeasures
[e_cryptanalysis_eh1.exam.xml Q_CRYPTANALYSIS_TYPES_01_EH1]