Lab Report 3 Date:2081/04/32

Experiment 1: Brute Force

Title: Programming to learn about Brute Force.

1. Objective:The objective of this Lab-Work is to use brute force attack is to gain unauthorized access to a system, account, or encrypted data by exhaustively trying all possible combinations until the correct one is found.
2. Theory: Brute force in the context of information security (IS) refers to a type of attack where an adversary systematically tries every possible combination of keys, passwords, or encryption solutions until the correct one is found. This method relies purely on computational power and time rather than exploiting weaknesses in the algorithm or encryption system.

2.1. Application of Brute force

a. Password Cracking

Objective: The most common use of brute force is to crack passwords to gain unauthorized access to systems, accounts, or devices.

How it works: A brute force attack systematically tries all possible combinations of characters (letters, numbers, symbols) until it finds the correct password. This can be applied to user login credentials, PINs, or any other password-protected systems.Example: Cracking a user’s password for online services or a local device (like a computer or mobile phone).

b. Cracking Encrypted Data

Objective: Brute force is used to decrypt encrypted data by testing all possible keys until the correct one is found.

How it works: In symmetric encryption (like AES) or asymmetric encryption (like RSA), brute force tries every possible key value to decrypt data.Example: An attacker may attempt to break into an encrypted file or email by guessing the encryption key.

c. Key Recovery in Cryptography

Objective: In cryptographic systems, brute force can be used to recover lost or forgotten encryption keys.

How it works: If a user has lost their encryption key but knows its structure (e.g., key length), brute force can be employed to systematically guess the key.

Example: An attacker or user attempting to recover access to encrypted backups or files when the key is lost.

d. Attacking Network Protocols

Objective: Brute force is sometimes used to break network protocols that rely on password-based authentication or encrypted communication.

How it works: In certain network security protocols (like WPA for Wi-Fi), brute force attacks attempt all possible keys until they discover the correct one.Example: Brute forcing the WPA/WPA2 password of a Wi-Fi network to gain unauthorized access.

e. Cryptanalysis

Objective: Brute force attacks are used as part of cryptanalysis efforts to evaluate the strength of encryption algorithms and break them.

How it works: Researchers or attackers might use brute force to test the resilience of an encryption method by attempting to decrypt ciphertext without knowing the key.Example: Testing the vulnerability of encryption algorithms, like DES (Data Encryption Standard), which have relatively shorter key lengths and can be cracked using brute force.

f. Breaking Hash Functions

Objective: Brute force can be applied to crack hash functions used in digital signatures or password hashing algorithms.

How it works: When passwords are hashed, brute force may be used to find the original input by matching the hash to the possible input combinations.

Example: Cracking password hashes in databases where weak hashing algorithms (like MD5 or SHA-1) are used.

1. Implementation of Brute Force.

*import string*

*import itertools*

*target\_password = input("Enter the password you want to crack:")*

*def brute\_force\_password(target):*

*chars = string.ascii\_lowercase*

*for length in range(1, len(target) + 1):*

*for attempt in itertools.product(chars, repeat=length):*

*guess = ''.join(attempt)*

*print(f"Trying: {guess}")*

*if guess == target:*

*return guess*

*return None*

*cracked\_password = brute\_force\_password(target\_password)*

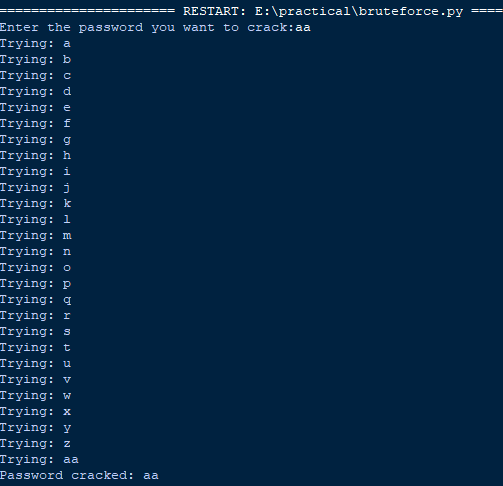
*if cracked\_password:*

*print(f"Password cracked: {cracked\_password}")*

*else:*

*print("Password could not be cracked.")*

Output:



Conclusion: In the above page we have learned about Brute Force and implemented them by using python.