Brute Force Password Attack on a Login API

Student Name:

Course: CYB444 - Computer Network Operations Security

Instructor: [Instructor's Name]

Date: [Insert Date]

Executive Summary

This project demonstrates a practical implementation of a Brute Force Password Attack targeting a login API hosted on localhost. The objective is to understand how unauthorized access can be achieved by systematically attempting different password combinations and to document the impact, process, and prevention mechanisms

1. Overview of the Attack

A brute-force attack is a method of systematically guessing a password by trying all possible combinations until the correct one is found. It is one of the most common types of password attacks and is effective when account protections like lockouts or rate limiting are not in place.

2. Attack Timeline

- T0: Attacker identifies login interface.
- T1: Script initiates multiple login attempts.
- T2: Server responds to each attempt (valid/invalid).
- T3: Correct password is found and access is granted.

3. Technical Details

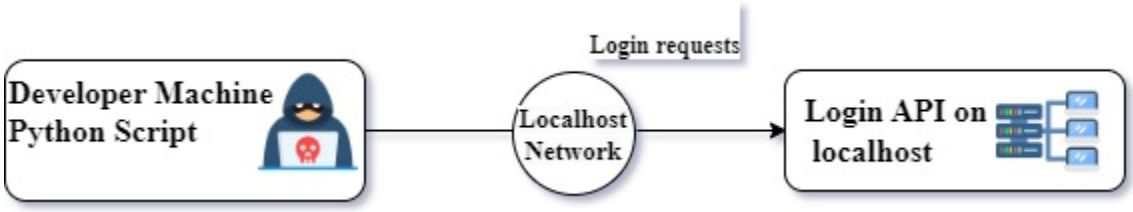
Type of Attack: Active

Threat Actor: Internal/External unauthorized user

Context: API testing environment (localhost)

Consequence: Unauthorized access to user account or system

4. Architectural Diagram



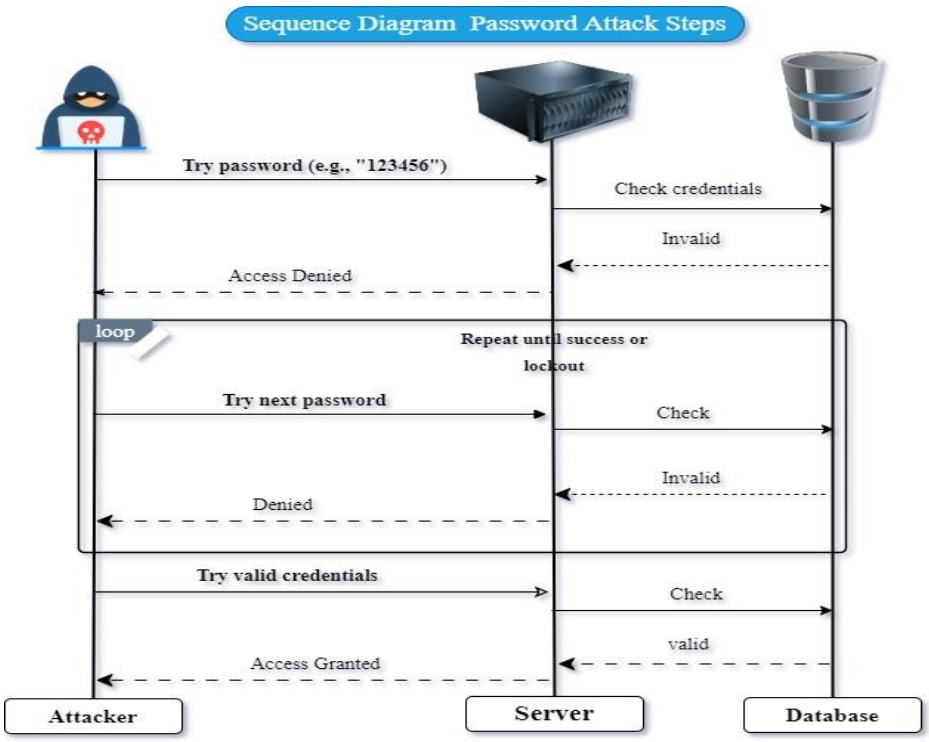
❖ Architectural Diagram

This diagram illustrates a brute force password attack setup within a local testing environment:

- **Developer Machine**: Runs a Python script to send repeated login attempts.
- **Localhost Network**: Represents the local environment where the attack is conducted.
- **Login API on localhost**: The target API that receives login requests and validates credentials.

The attacker sends multiple login attempts through the local network, trying different passwords until the correct one is found.

5. Sequence Diagram



❖ Sequence Diagram

This diagram illustrates the step-by-step flow of a brute-force password attack:

- The attacker sends a login request with a guessed password.
- The server checks the credentials against the database.
- If the password is invalid, access is denied.
- The attacker repeats the process with the next password.
- Once a valid password is found, access is granted.

The process continues in a loop until successful login or lockout occurs.

6. Tools and Technologies

- Programming Language: Python
- Library Used: requests
- Target Environment: Localhost API
- Login API Endpoint: http://localhost:8000/login

7. Attack Steps (Code)

[Insert code block here]

8. Screenshots & Results

Include screenshots of the terminal running the attack script and showing success, as well as the affected login interface.

9. Summary

This project demonstrates a fundamental brute-force attack on a login interface. It highlights the ease with which systems lacking basic security protections can be compromised.

10. Insights and Discussion

- ✓ Importance of implementing account lockouts and rate-limiting.
- ✓ Necessity of using multi-factor authentication.
- ✓ Security must be tested even in development environments.

11. References

1. OWASP Foundation. (2023). "Brute Force Attack." https://owasp.org/

2. Kaspersky. (2023). "Password Attacks Explained."

3. Python Requests Library Documentation. https://docs.python-requests.org/