LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No. 2**

**A.1 Aim:**

To implement a password strength checker

**A.2 Prerequisite:**

Understanding of Authentication methods

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Appreciate the importance of proactive password checking.

2. Can able to comprehend how vulnerable the system could be if password selection is done incorrectly.

**A.4 Theory:**

Authentication is the process of binding of identity to a subject. This process validates the users credentials and determines whether the user is allowed to access a system or a resource or not. The authentication information comes from one or more of the following

* + What entity knows (*eg.* password)
  + What entity has (*eg.* badge, smart card)
  + What entity is (*eg.* fingerprints, retinal characteristics)
  + Where entity is (*eg*. In front of a particular terminal)

An authentication process consists of obtaining authentication information, analyzing the data and determining if it is associated with that entity.

Passwords are the most common mechanism used for authentication mainly for two reasons: ease of use and simple. However it suffers from many problems such as the user may forget the password; an attacker may know the password and replay the password.

The authentication system using passwords should have mechanism that enforces the user to select strong or good passwords. The aim of the system should be that the attacker should take lot of time to crack the password.

A strong password must have the following components:

At least one uppercase letter

At least one lowercase letter

At least one numeric digit

At least one special character

String length should be of at least 8 characters

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No. | Name: |
| Class | Batch: |
| Date of Experiment: | Date of Submission: |
| Grade: | |

**B.1 Software Code written by student:**

***(Paste your Java code completed during the 2 hours of practical in the lab here)***

**B.2 Input and Output:**

***(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)***

**Input:**

1. Input string acting as password

**Output:**

Output screenshots with different cases

**B.3 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

**B.4 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)***

**B.5 Questions of Curiosity**

***(To be answered by student based on the practical performed and learning/observations)***

Q1: Discuss the various attacks on passwords

Q.2 Explain some other authentication methods in brief.