SVKM'S NMIMS (Deemed-to-be University)
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT AND ENGINEERING
MUMBAI CAMPUS

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. A016	Name: Varun Mahendra Khadayate
Class Btech CsBs Third Year	Batch: 1
Date of Experiment:24-12-2021	Date of Submission: 24-12-2021
Grade:	

B.1 Software Code written by student:

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

```
lower, upper, special, digit = 0, 0, 0, 0
password = input("Enter your password:: ")

if (len(password) >= 6):
    for i in password:

        for word in password.split():
            if(word[0].isupper()):
                upper += 1

        if(i.islower()):
            lower += 1

        if(i.isdigit()):
            digit += 1

        if(i == '@' or i == '$' or i == '_' or i == '#' or i == '&' or i == '*' or i == '^'):
            special += 1

else:
    print("Password should be more than 6 characters")
if (lower >= 1 and upper >= 1 and special >= 1 and digit >= 1):
    print("Valid and Strong Password")
else:
    print("Invalid and Weak Password")
```

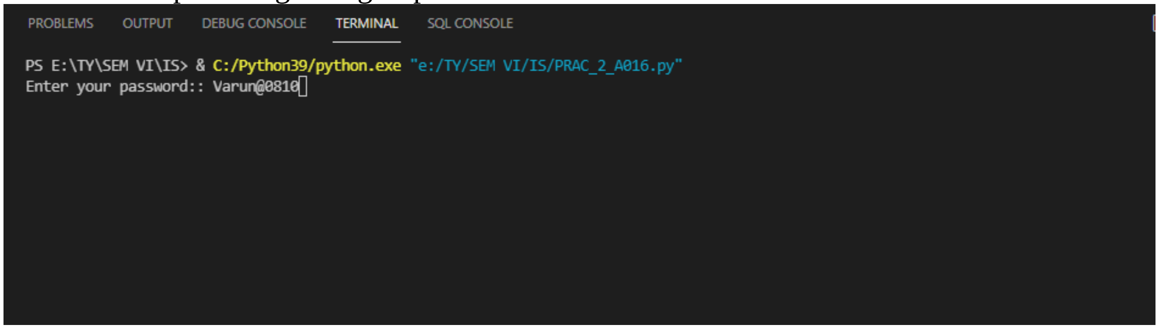
B.2 Input and Output:

(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:

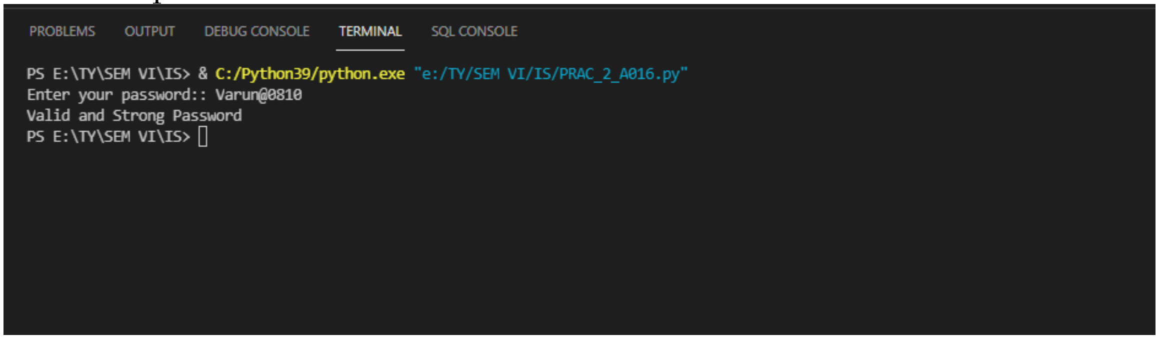
1. Input string acting as password



```
PS E:\TY\SEM VI\IS> & C:/Python39/python.exe "e:/TY/SEM VI/IS/PRAC_2_A016.py"
Enter your password:: Varun@0810
```

Output:

Output screenshots with different cases



```
PS E:\TY\SEM VI\IS> & C:/Python39/python.exe "e:/TY/SEM VI/IS/PRAC_2_A016.py"
Enter your password:: Varun@0810
Valid and Strong Password
PS E:\TY\SEM VI\IS>
```

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)

We were able to understand the following points to keep in mind for password checker functioning

1. At least one uppercase letter
2. At least one lowercase letter
3. At least one numeric digit
4. At least one special character
5. String length should be of at least 8 characters

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)

Hence, we were able to implement a password strength checker using Python.

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

1. Phishing

Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device. We highlight several examples on the OneLogin blog.
Here are a few examples of phishing:

- **Regular phishing**. You get an email from what looks like goodwebsite.com asking you to reset your password, but you didn't read closely and it's goodwobsite.com. You "reset your password" and the hacker steals your credentials.
- **Spear phishing**. A hacker targets you specifically with an email that appears to be from a friend, colleague, or associate. It has a brief, generic blurb ("Check out the invoice I attached and let me know if it makes sense.") and hopes you click on the malicious attachment.
- **Smishing and vishing**. You receive a text message (SMS phishing, or smishing) or phone call (voice phishing, or vishing) from a hacker who informs you that your account has been frozen or that fraud has been detected. You enter your account information, and the hacker steals it.
- **Whaling**. You or your organization receive an email purportedly from a senior figure in your company. You don't do your homework on the email's veracity and send sensitive information to a hacker.

2. Man-in-the-middle attack

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords. If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle. Similarly, in 2017, Equifax removed its apps from the App Store and Google Play store because they were passing sensitive data over insecure channels where hackers could have stolen customer information.

3. Brute force attack

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

4. Dictionary attack

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

5. Credential stuffing

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

6. Keyloggers

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

Q.2 Explain some other authentication methods in brief.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines, or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or a passport.

The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

Users provide their digital certificates when they sign into a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.

4. Biometric authentication

Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Here are key advantages of using biometric authentication technologies:

- Biological characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication methods include:

- **Facial recognition**—matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar, like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.
- **Fingerprint scanners**—match the unique patterns on an individual's fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people's fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers, despite their frequent inaccuracies. This popularity can be attributed to iPhones.
- **Speaker Recognition** —also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities. A voice-protected device usually relies on standardized words to identify users, just like a password.
- **Eye scanners**—include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the colored ring around the pupil of the eye. The patterns are then compared to approved information stored in a database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses.

5. Token-based authentication

Token-based authentication technologies enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission. Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.