import re

def assess\_password\_strength(password):

# Define password strength criteria

length\_criteria = len(password) >= 12

uppercase\_criteria = bool(re.search(r'[A-Z]', password))

lowercase\_criteria = bool(re.search(r'[a-z]', password))

number\_criteria = bool(re.search(r'\d', password))

special\_char\_criteria = bool(re.search(r'[!@#$%^&\*(),.?":{}|<>]', password))

# Count criteria met

criteria\_met = sum([

length\_criteria,

uppercase\_criteria,

lowercase\_criteria,

number\_criteria,

special\_char\_criteria

])

# Assess password strength

if criteria\_met == 5:

strength = "Strong"

feedback = "Your password is strong and secure."

elif criteria\_met == 3 or criteria\_met == 4:

strength = "Medium"

feedback = "Your password is okay, but consider adding more diversity (e.g., special characters or more length)."

else:

strength = "Weak"

feedback = "Your password is weak. Use at least 12 characters, including uppercase, lowercase, numbers, and special characters."

# Return the result

return {

"password": password,

"strength": strength,

"feedback": feedback

}

# Test the tool

if \_\_name\_\_ == "\_\_main\_\_":

password = input("Enter a password to assess its strength: ")

result = assess\_password\_strength(password)

print(f"Password: {result['password']}")

print(f"Strength: {result['strength']}")

print(f"Feedback: {result['feedback']}")