Name:– Krishnmohan Mishra MSc CS F016

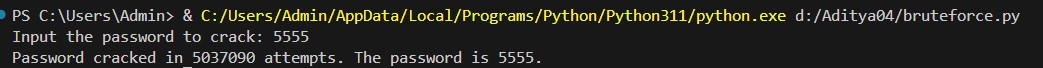
Cyber Security

# Practical 4: Implement Brute force Attack and Virus

Brute Force Input:

|  |
| --- |
| import itertools import string  def bruteforce(password):  chars = string.printable.strip() attempts = 0 for length in range(1, len(password) + 1): for guess in itertools.product(chars, repeat=length):  attempts += 1 guess = ''.join(guess) if guess == password:  return (attempts, guess) return (attempts, None)  password = input("Input the password to crack: ") attempts, guess = bruteforce(password) if guess: print(f"Password cracked in {attempts} attempts. The password is  {guess}.") else:  print(f"Password not cracked after {attempts} attempts.") |

Brute Force Output:



Virus Input (Creating file and deleting it):

|  |
| --- |
| import os import time def create\_files(directory): if not os.path.exists(directory):  os.makedirs(directory)  for i in range(5):  file\_path = os.path.join(directory, f"malicious\_file\_{i}.txt") with open(file\_path, 'w') as file:  file.write(f"This is a simulated malicious file {i}.") print(f"Created: {file\_path}")  def delete\_files(directory): if os.path.exists(directory): for file\_name in os.listdir(directory):  file\_path = os.path.join(directory, file\_name) if os.path.isfile(file\_path):  os.remove(file\_path) print(f"Deleted: {file\_path}") os.rmdir(directory) print(f"Deleted directory: {directory}")  if \_\_name\_\_ == "\_\_main\_\_":  test\_directory = "D:\Test"  print("Simulating malicious behavior...") create\_files(test\_directory)    # Simulate waiting time time.sleep(10) # 10 seconds    delete\_files(test\_directory)  print("Simulation completed and cleaned up.") |

Virus Output:

