Case Western Reserve University

Department of Computer and Data Sciences

EECS 349&444: Computer Security

Assignment Date:	09/19/2019
Sumission Date:	09/24/2019
First Name:	
Last Name:	
Google Drive Link:	
Abstract of the feedback:	

* This is the second half-part of HW1 which contains 20 points. You are encouraged to finish by group. Any submitted work that it copied from any source or too similar to be an independent write-up will not be given credit. Please submit this homework (e-copy) on SIS by 11:15am on 09/19/2019.

Buffer Overflow Practice: Flight Ticket Purchase

Problem 1 (20 pts: 10pts/sub-step). Crack the passwords to enter the ticket purchase system.

Step 1: Cracking Passwords

- **It's two-step process to crack the passwords to enter the ticket purchase system:**

1. **Social engineering**

The unzip password contains characters from the following categories with the length of 8 characters:

- Choose 1~2 words from the word list provided
- Base 10 digits (0 through 9)
- Non alphanumeric characters: @$

Word List

CWRU; CDS; Case; Janie; Jack; Puppy; Love; Euclid; Ohio; Paris;

You are allowed to ask 10 questions answered with Y/N, for example:

- Does the characters come from the first word?
- Is the first character "C"?
- Does your password include @ symbol?
- ……

2. **Attack utilizing buffer overflow to enter the system**

Problem 2 (20pts). Exploiting the buffer overflows to purchase your ticket.

Step 2: Hacking the system to purchase tickets

- The current balance in your banking account is **$480**, but the price for each ticket is **$500.** You need to exploit the buffer overflow of the software for ticket purchase.

Problem 3 (20pts). Exploiting the buffer overflows to upgrade your ticket.

Step 3: Upgrade your Economy to First class

- After you successfully purchase the tickets, you will be asked to input your information for check-in. Please exploit the buffer overflow to upgrade your **economy** class to **first** class for free.

Requirement: For each step, when you successfully exploit the vulnerabilities to perform buffer overflow attacks, please (1) provide your solution; (2) provide the screenshot(s); and (3) explain how you get the solution (i.e., what kinds of buffer overflows exist, how you exploit them, etc.).