UNIVERSITY OF WAIKATO

COMPX304-19B—Advanced Networking and Cyber Security

Lab 8—Buffer Overflow Vulnerabilities and Attacks

Problem Description

The only thing that computers do is manipulate numbers. The same applies when dealing with the structure of an application. Variables are offsets, types are sizes, pointers are numerical identifiers, etc. As discussed in class, an application's call stack contains all the information necessary for that function to run and enable the successful continuation of the program back to the function it called it. If information is copied without checks, the self-imposed barriers between memory objects break down: information can be leaked or tampered with or (in the best case) the application might crash. These type of attacks are called buffer overflow attacks.

Part 1

Study the attached lab8.c code. (A) Perform an availability attack that crashes the application. (B) Perform a confidentiality attack, such that a non-admin user is granted privileged access. Show your methods to the lab marker and explain how they work.

Part 2

The lab8.c code contains numerous vulnerabilities that enabled this type of attacks. Each one might had not been a threat individually but together, they enabled this exploit to take place. First, identify each vulnerability in this chain; second, patch the lab8.c code with appropriate fixes, such that buffer overflow attacks cannot succeed.

At your Leisure

A more sophisticated buffer overflow attack, called "return-to-libc"[1] can overwrite the whole contents of a stack frame such that everything is the same except the return address. Thus, when the function under attack finishes, it returns to a code address different than the one who called it! This can be drastically elevated if the function returns to another sensitive function. Engineer code and inputs that enable such an attack; identify the various defenses set in place by the compiler and operating system to prevent it from happening.

----------Lab 8 Ends----------

[1] https://en.wikipedia.org/wiki/Return-to-libc_attack