CSE4501 – Vulnerability Research: Lab 3

Eric Pereira

Septemer 24th, 2019

Contents

Use the necessary tools to perform an analysis of the binaries provided. You can explore the source code and use Makefiles to new binaries. Please submit write-ups of your analysis. Your points will be based on completeness of analysis, your understanding of the problems, and if you were able to achieve the goals. Each problem is worth 20 pts for a total of 40 pts.

Problem 1

Very similar to the example in lecture. Source code is available for assistance. A pre-built binary is included and your automated exploit should work against this Binary. Binary should have all mitigations, including ASLR and stack canaries (Makefile is included). Confirm you have enabled ASLR in Linux by running `cat /proc/sys/kernel/randomize_va_space` (result should be '2'). If it is not, you can enable it by running `echo 2 > /proc/sys/kernel/randomize_va_space` as the root user.
Solution:

Problem 2

Exploitation of UAF C++ object, as discussed at the end of the lecture slides. Understanding of vtables/vptr is required. ASLR is not required for this lab, and should be disabled (value of 0 in `/proc/sys/kernel/randomize_va_space`)