430/530 – Buffer Overflow Lab

Name: Jacob Boicken

ASLR

Cite any sources used to assist you with your answers.

Briefly describe what ASLR is/does and what purpose it serves.

A buffer overflow is when a program essentially does not bounds check a user input or operations that a user can influence. This leads to the program writing to memory outside of the designated space / memory buffer for data to be written to. This can be used to write over the program code with malicious payload code. The attacker needs to know where the code is to overwrite though. Address Space Layout Randomization is security technique that randomizes where the stack, heap, and code are in the memory space for the process each time it is run. This makes it highly unlikely for an attacker to be able to place malicious code in the correct memory as the code is located in different areas of memory.

https://www.howtogeek.com/278056/what-is-aslr-and-how-does-it-keep-your-computer-secure/

Determine if your Kali VM in ISELab is using ASLR. Justify your answer, i.e., explain how you know ASLR is being used on your Kali VM. It may be helpful to provide a screen capture to supplement your answer.

Yes, the picture below shows that the VM has the kernel parameter of "randomize_va_space" set to the value 2. This according to both sites below enables process address space randomization. The value of 1 for this parameter means that the code, libraries, and stack are all randomized. Then, the value of 2 means that the heap is randomized in addition to what is for the value of 1.

This means that programs run in the kali box have ASLR for all process heap, stack, code, and linked libraries.

https://sysctl-explorer.net/kernel/randomize_va_space/
https://www.kernel.org/doc/Documentation/sysctl/kernel.txt

Insert Image

Lab Setup

message file

overflow.c code

Experiment 1

Insert Image

Experiment 2

Insert Image

Experiment 3

Insert Image

Experiment 4

Insert Image

Reminder: If, *at any point* during this lab, you get an error message, such as ‘cat: message: No such file or directory,’ 'command not found,’ or 'sh: 1: <something> not found,’ **something is incorrect**, and you will lose points if you do not correct it. You need to debug your program, check your file locations, and check your terminal commands. If you need help diagnosing the problem, contact your TA(s). Please check your images before submitting your PDF.

Lab Reflection

Remember, answer using complete sentences and enough details/specifics to avoid vague answers. Please spend time thinking of a thoughtful response. You may use outside sources to develop your responses but be sure you cite any sources you use.

A. Coding with security in mind and using ASLR are two buffer overflow mitigation strategies discussed in this lab. What are two other ways buffer overflow attacks could be mitigated?

B. This lab mentioned the Morris Worm and Heartbleed. Perform Internet research to find another prominent buffer overflow attack. Provide a brief description of the attack and include information such as the attack name, where the buffer vulnerability exists (e.g., specific piece of software, OS, protocol), a CVE number, and how the attack unfolds.

C. In a paragraph of *at least* five sentences, reflect on what you have accomplished in this lab.