Ryan Randazzo

CECS 478 Sec 02

Dec. 11th, 2022

Lab 4 Buffer Overflow

For this lab I installed Linux Mint 17 in Oracle Virtualbox. Once getting the files to the VM, I ran readelf -s vuln to see relevant addresses connected to the vuln.c file.

Graphical user interface, text

Description automatically generated

From here I found addresses to key functions in the file.

readelf -s vuln -> 080485ad bof, 080485cf main, 08048695 dummy\_function

(gdb) x $ebp -> 0xbfffed38: 0xbffff148 3221221704

(gdb) x &buffer -> 0xbfffeccc: 0xb7fdc4a0 3086861472 -= 134,360,232

I read the Smashing the Stack for Fun and Profit article and watched several youtube videos to try to understand how to complete this lab and how to properly make the exploit.c file.

From here I made my exploit.c file using the addresses I found in order to overflow the stack and use the shell code I created to override the file, changing the Input size from 0 to 517 for the output.

Graphical user interface, text

Description automatically generated

During the lab, I encountered numerous setbacks with setting up my VM and essentially wasting my time attempting to set up a shared folder between the guest Linux VM and my host computer. I could not get the exploit.c file to properly work and jump to the root user, but I was able to overload the stack for the smash attack.