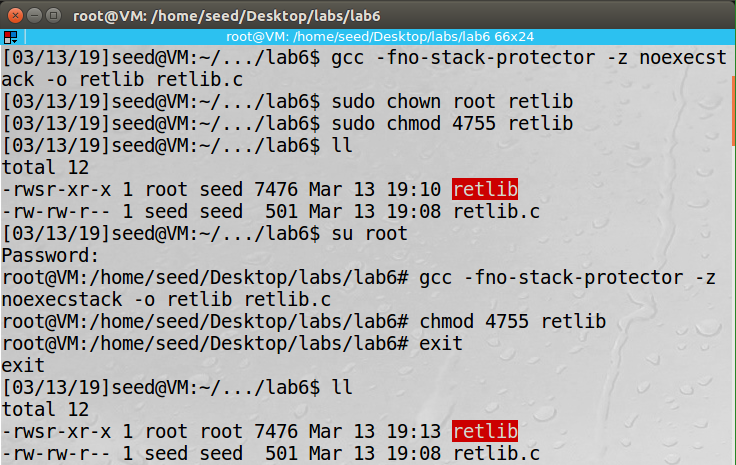
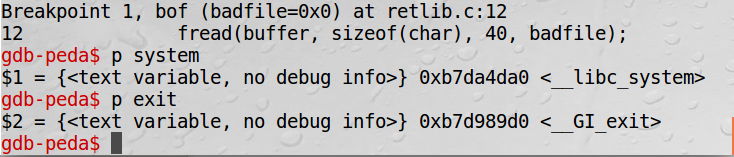
Lab 6 Report – Austin Adams – CS 445

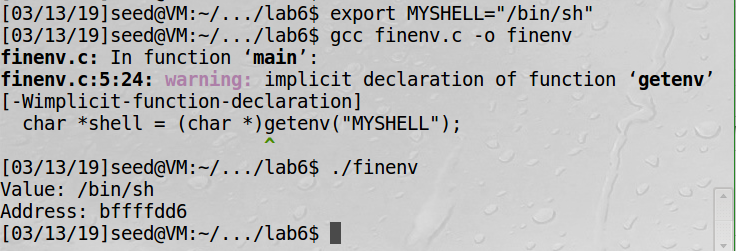
Task 1: We need to make our program a set-UID program with a buffer overflow error. Using sudo the owner group was seed but using the instruction provide in the lab made the owner group root. This didn’t change the results both files worked.



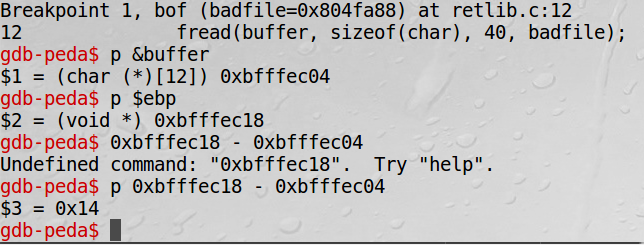
Next we need to find the addresses of the system and exit function, so we can add them to our bad file. (Note: the addresses are different from what is in the actual file because I took this snapshot from my laptop)



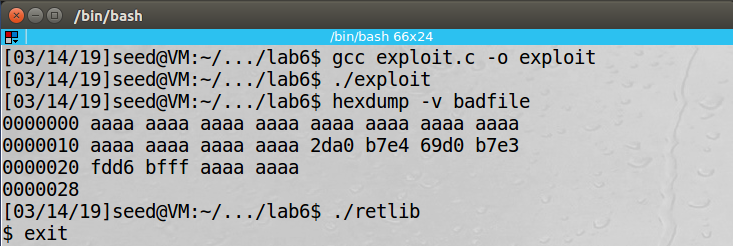
Then we export our environment variable containing the /bin/sh. However after running it the first time I realized that I shouldn’t have added the quotation marks.

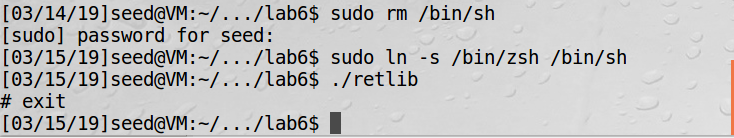


After getting the needed addresses we need to know where to place them in the badfile so we get the distance from the buffer to the ebp and in my case it was 0x14 or 20. As for the X, Y, and Z values I knew that system call would need to replace the original return address. Then the exit call would have to be next because the system call would be replace with some value from the ebp and the next address on the stack would be the system calls return address. (When the system call finishes the next thing on the stack would be it return address and to avoid suspicion well call the exit function.) Finally for the /bin/sh I knew that parameters for the system call should be stored at ebp + 8.

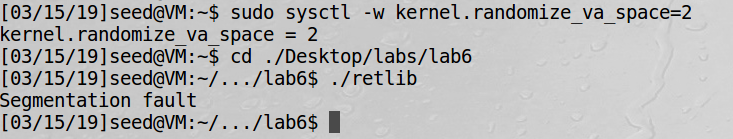


When I first ran it I noticed that I was giving me the seed shell instead of the root shell I then realized that I was running this in the /bin/bash which has protection against these attacks. After changing the the shells to /bin/zsh like we did in the buffer overflow attacks I got the root shell.





Task 2: With the memory randomizer on the addresses for the system(), exit(), and buffer would change every time you run the program.



Task 3: With the stack guard in place it would detect the buffer overflow on the stack and abort the process.

