CSCD 437
Lab 3
Buffer Overrun

ARTICLES TO READ:

1) Read the article Dr_Dobbs-Anatomy_of_a_Stack_Smashing_Attack_and_How_GCC_Prevents_It.pdf which can be found in Modules
2) Read the article Smashing_the_Stack_for_Fun_and_Profit.pdf which can be found in Modules
3) Read the article Return-into-libc_without_Function_Calls.pdf which can be found in Modules

SPECIFICATIONS COMPLETED ON A UBUNTU VM

1) If you didn't use a virtual machine for Lab 1 then you will need to download and install VirtualBox
2) Download and install Ubunutu 20.04 LTS. (Ensure you allow at least 20 gigs of hard drive space)
3) This might help with some of the stack protections https://stackoverflow.com/questions/2340259/how-to-turn-off-gcc-compiler-optimization-to-enable-buffer-overflow
4) Turn off ASLR with `echo 0 | sudo tee /proc/sys/kernel/randomize_va_space`
5) Compile stackOverrun.c -o stackOverrun
    a. You will need to turn stack protection off with `-fno-stack-protector`
    b. You may have to modify other protections
6) Run the executable from stackOverrun
    a. Note: You will need to pass the executable a String
    b. Note: Note the address of the bar function
    c. Note: The Borland compiler is 32 bits and Ubuntu gcc compiler is 64 bits
7) Run perl hackOverrun.pl
    a. Change the $args line for the string and the address
    b. Note: You may need to pad the initial set of letters in hackOverrun.pl to overflow to the return address location on the stack
    c. Note: This lab presumes hackOverrun and stackOverrun are in the same directory

NOTE

- The only changes you can make to stackOverrun.c is to add more %p\n to the following two printf statements in the *foo* function.
    - printf("My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n\n");
    - printf("Now the stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n\n");
- The only line you can change in HackOverrun.pl is:

```
$args = "ABCDEFGHIJKLMNOP"."\x90\x11\x40";
```

EXTRA CREDIT

- Instead of printing to the screen in the bar function actually inject code that opens a terminal. This is not as simple as you think it is.
- Don't attempt the extra credit without everything else working properly.
- You can't use the system command or any system calls.

WHAT TO TURN IN:

As a team, submit a zip containing:

- Output captures in a single PDF that show your exploit worked/didn't work in Ubuntu. Note: There will be output in either case of it worked or didn't work. PDF is named team number.pdf (Example: team16.pdf)
- Screen captures of hackOverrun.pl and stackOverrun.c in the single pdf
- The hackOverrun.pl and stackOverrun.c files
- Included in code.pdf should be a narrative explaining:
    - settings you had to turn off

- struggles you had/websites you used
- Your process to getting the buffer overrun to work properly. If you couldn't get it to work then a narrative explaining what happened and what needs to be done so it might work.

Name your zip your team numberLab3.zip (Example: team16Lab3.zip)