Assignment 3: Team - Buffer Overrun exploit

Published

-compile and run StackOverrun.c: StackOverrun.c
-note the address of the bar function
-add that address to HackOverrun.pl (remember to put the address in in reverse order): HackOverrun.pl
-note that you may need to pad the initial set of letters in HackOverrun.pl to overflow to the return address location on the stack
-You'll need a Perl interpreter to run the Perl script on the windows side. ActivePerl is a good free one for windows
-You must implement the exploit with **TWO** different compilers. The in class example used the Borland C++ command line compiler: borland_compiler.zip The exploit can also be implemented with gcc, but depending on the version and platform on which you run you might need to turn of stack protection with: *-fno-stack-protector*

Provide output captures that show your exploit worked with two different compilers. In a README.TXT, specify which compilers you used and on what OS you ran your code. Submit a zip file with your results (output captures, associated source code, README.TXT, etc.). Be sure and include team member names as part of your submission.

Below is an excellent link to discussion of how gcc works to protect the stack. The link also contains excellent discussion of how buffer overrun works.

http://www.drdobbs.com/security/anatomy-of-a-stack-smashing-attack-and-h/240001832?pgno=1 (http://www.drdobbs.com/security/anatomy-of-a-stack-smashing-attack-and-h/240001832?pgno=1)

15 Extra points will be given if your exploit includes a payload and you can get that payload to execute and spawn a shell (command prompt).

Have fun!

Points	40
Submitting	a file upload
File Types	zip

Due	For	Available from	Until

Due	For	Available from	Until
Oct 5, 2018	Everyone	-	-