

I am getting a “public key denied” or some other authentication error. What should I do?

Read the SSH+SCP Guide. All answers/guides for ssh problems are there.

I am getting a segfault in gdb when I try to set breakpoints.

Please, re-read the assignment. In particular, this part:

When running gdb using these command line flags, be sure to first issue 'catch exec' then 'run' the program before you set any breakpoints; the command 'run' naturally breaks the execution at the first execve call before the target is actually exec-ed, so you can set your breakpoints when gdb catches the execve. Note that if you try to set breakpoints before entering the command 'run', you'll get a segmentation fault.

spl0it0 doesn't work if I take it from the section slides.

Did you add any other code (like declaring other local variables in main)? If so, make sure that only the buffer is declared in the main of your spl0it0.c. The shellcode variable is included with the #include at the beginning of the skeleton. If you didn't use the included shellcode but tried to write your own or you declared any other local variables in your spl0it0.c, then the layout of the stack may be different, so the exact addresses from section won't work. Either try to figure out what the new address of the shellcode location is or make sure your code is *really* the same as that from section.

After I fixed a bug my exploit starting working strangely

Changing the input size of your string can, in some cases, change the layout of the stack. This will cause the addresses of everything to change. If you fix the size of your input string, you'll stop having stack layout changes. (We set this up in a way that minimizes the layout changes, but can't eliminate them entirely.)

How can I see the entire program in assembly?

Objdump is a useful tool for this, e.g. `objdump -d targetN`

-d is for 'disassemble all code'

-D is for 'disassemble everything, even if its not code'