Interestingly enough, the default compile settings in VS2017 don’t enable ASLR. The main function is the same address every time.

Do To:

* What is a stack cookie
* What is a format string vulnerability
* How can we use that to know the address for the system function in windows.h
* Exploit to bypass DEP

Next week

* Compile with ASLR
* Calculate offset with format string
* Perform buffer overflow