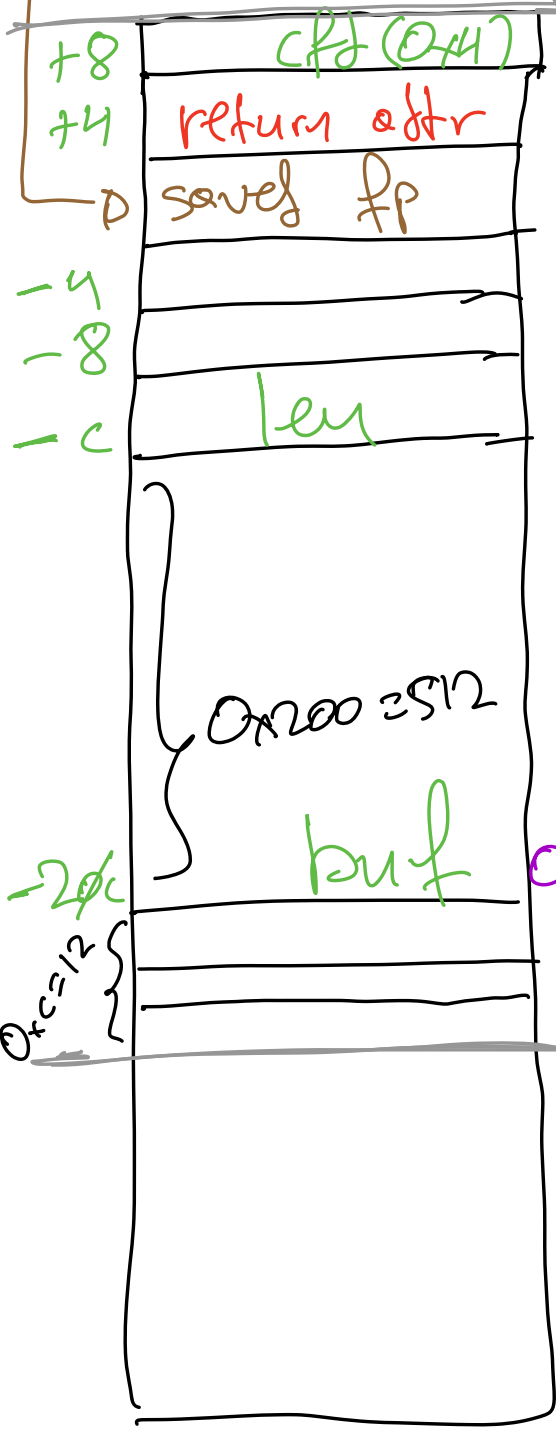


Code Injection

%ebp

(PCLi-hub)
stack frame



0xbffffd5c

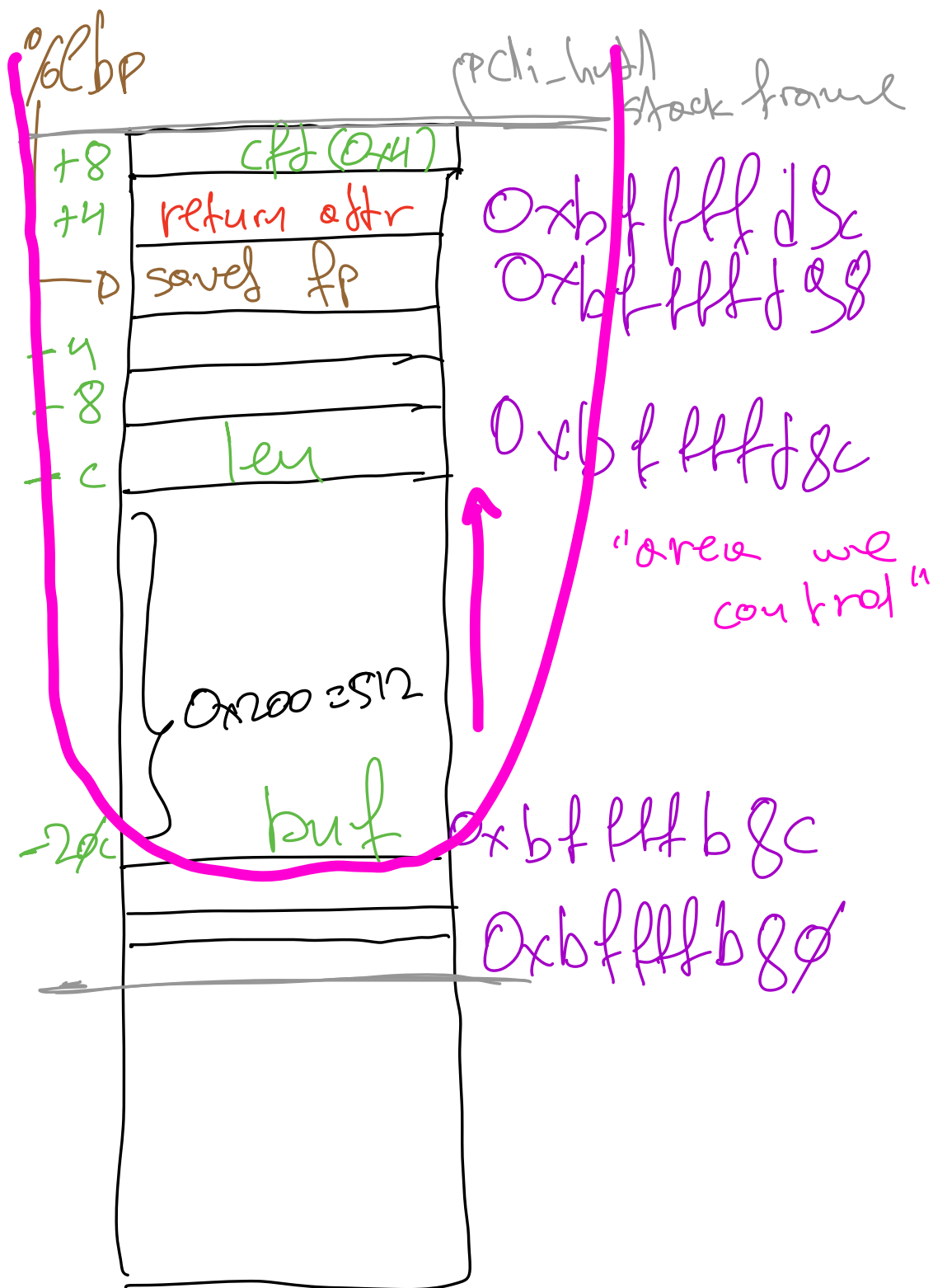
0xbffffd38

0xbffffd3c

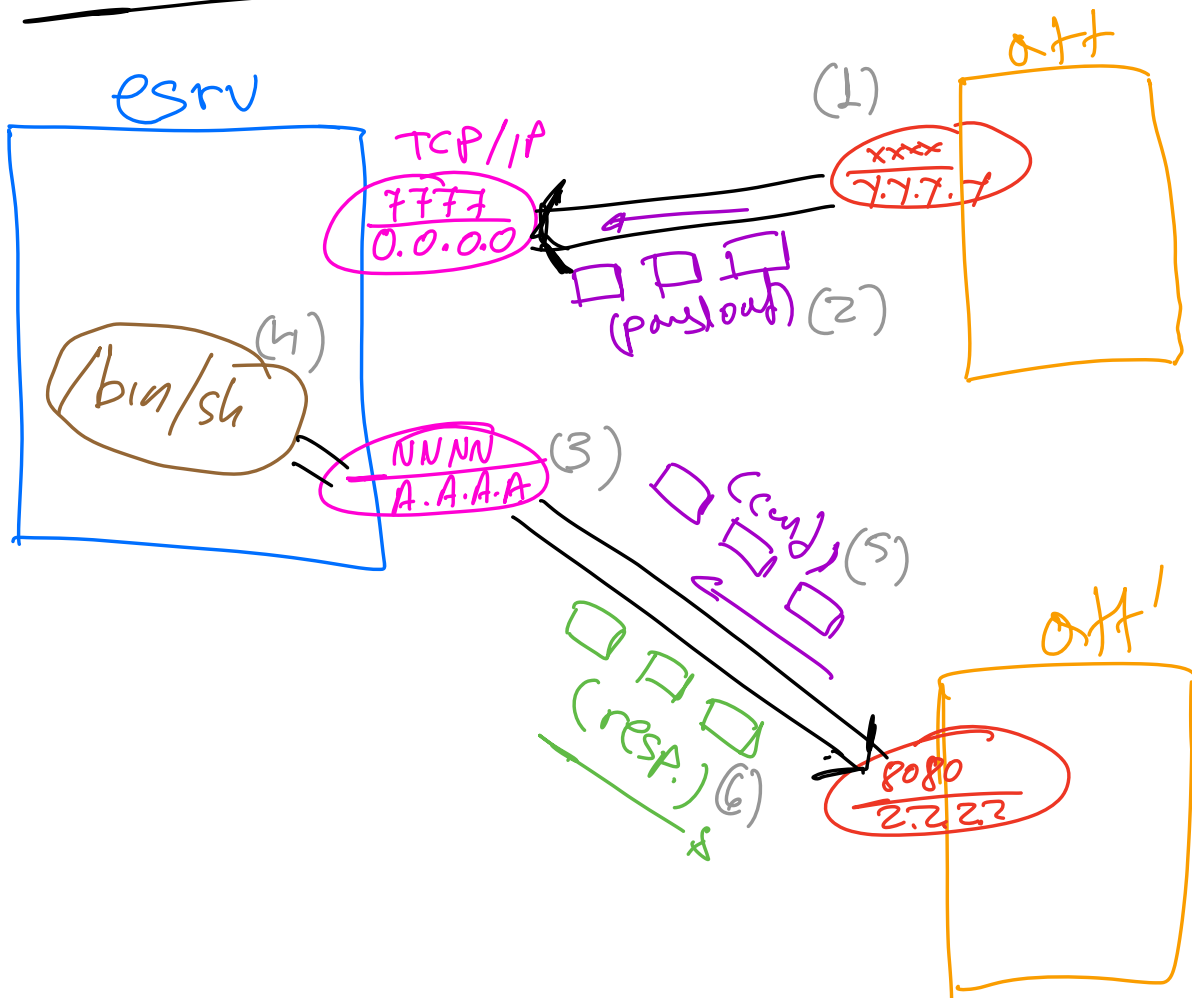
0xbffffb8c

0xbffffb80

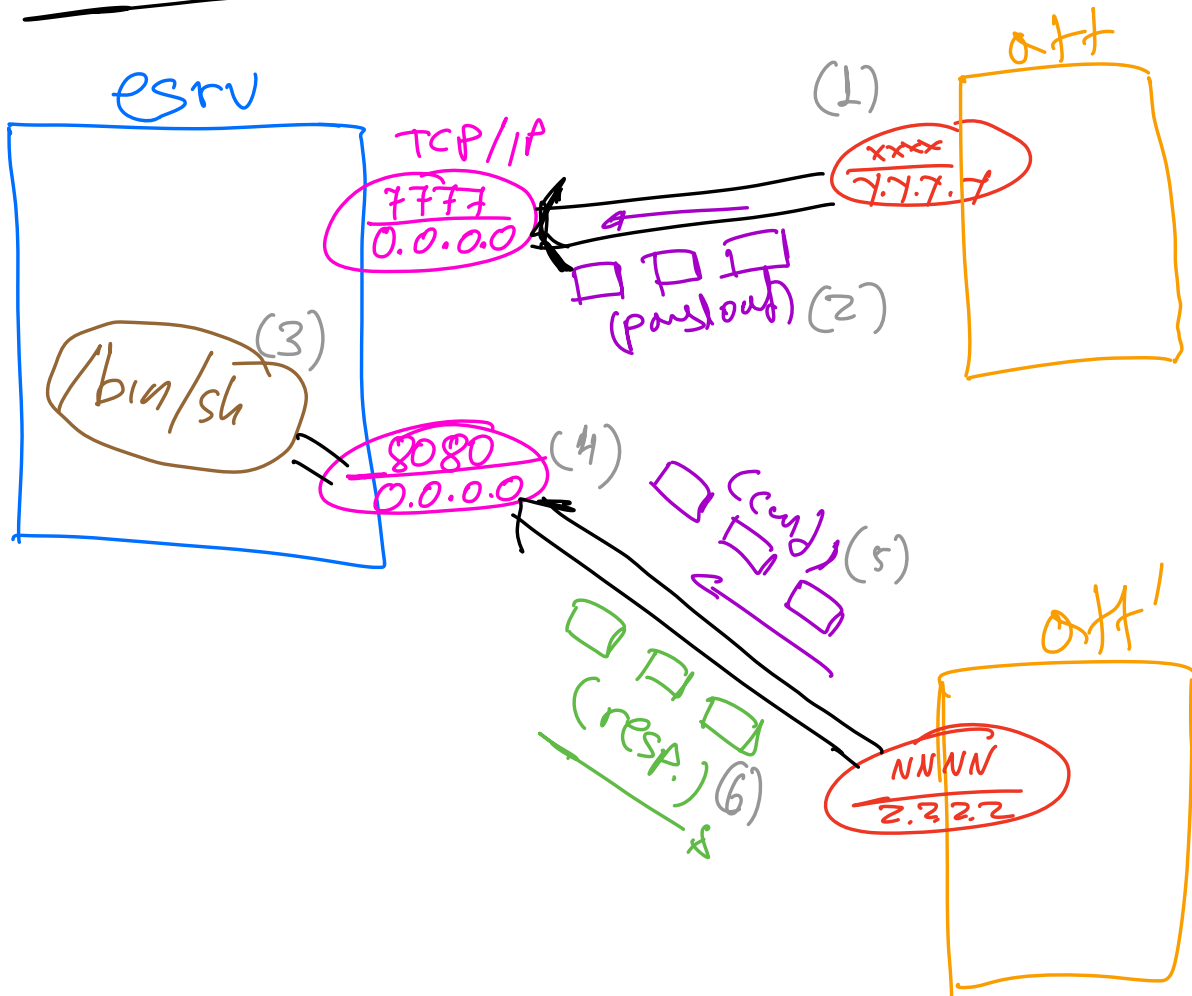
0x218=536



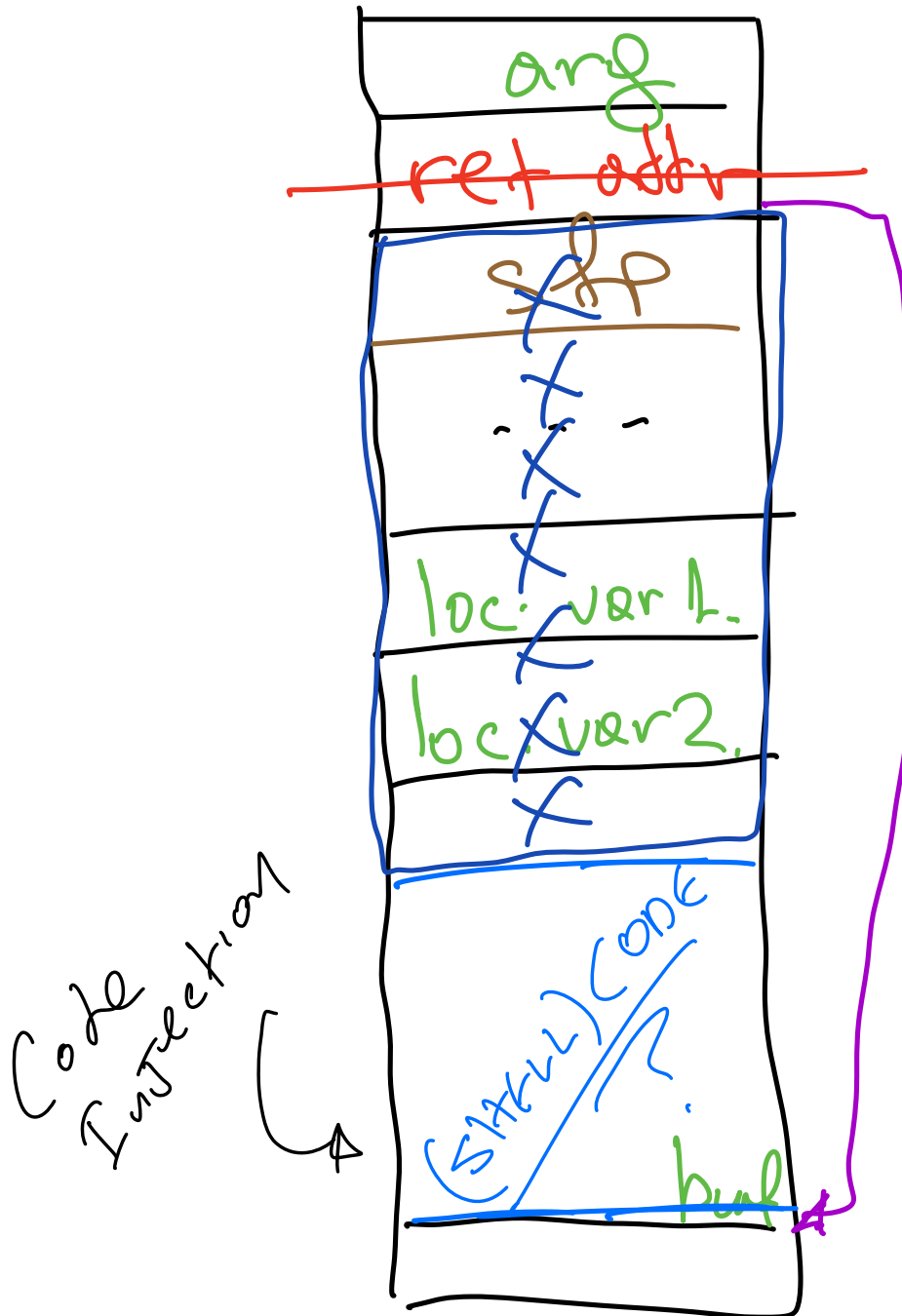
Deverse Shell

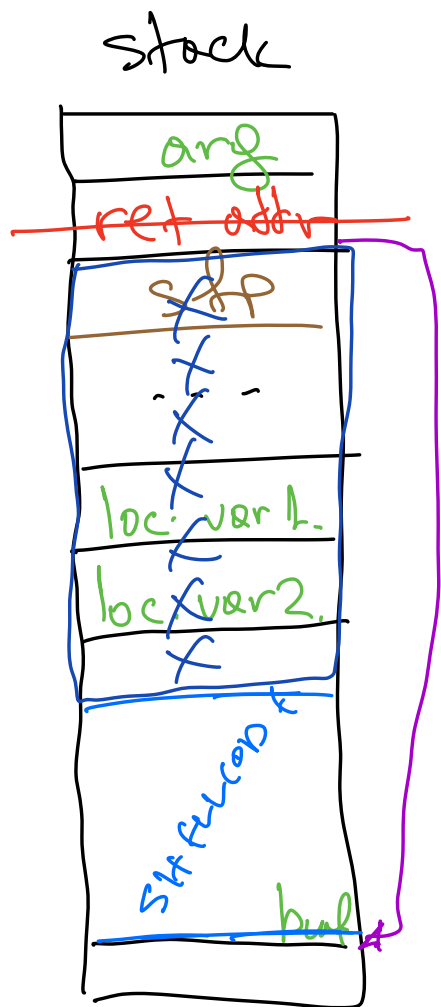


Bind Shell

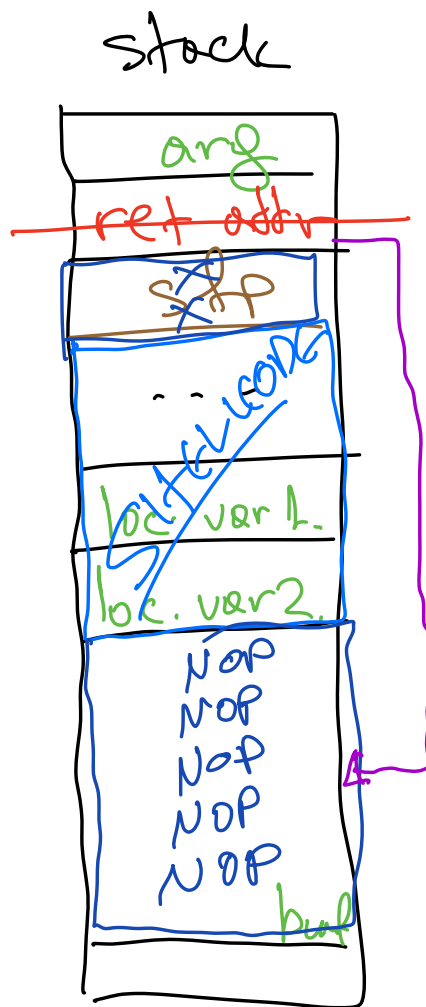


stack



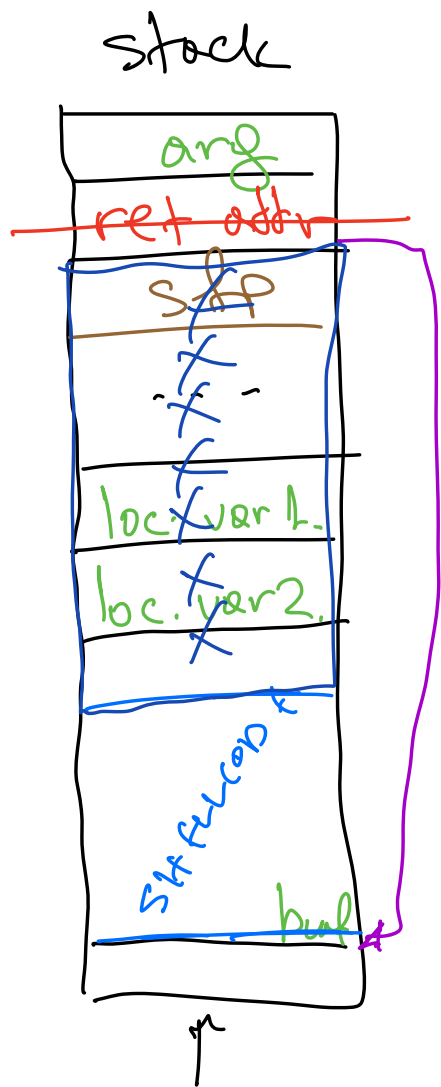


↑
Traditional
code injection

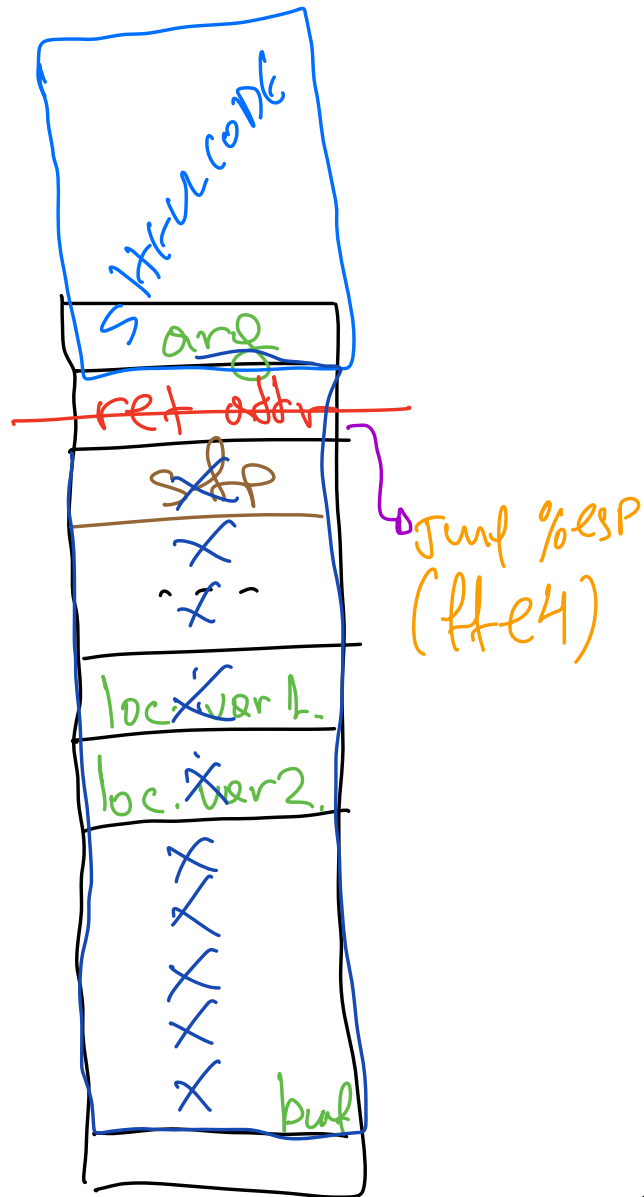


↑
NOP-sled-based
code injection

VS.

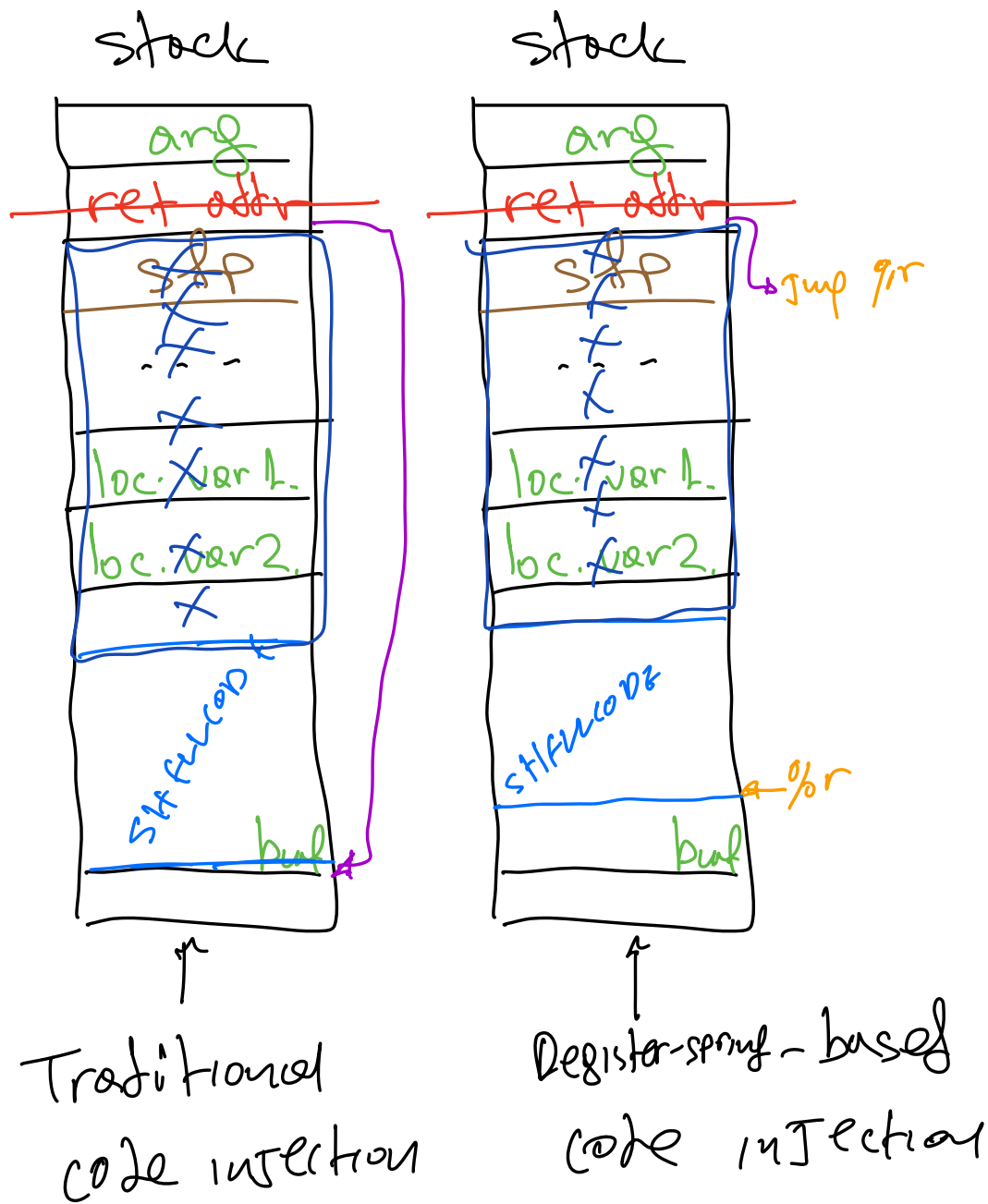


Traditional
code injection



Jump %esp - based
code injection

vs.



vs.

