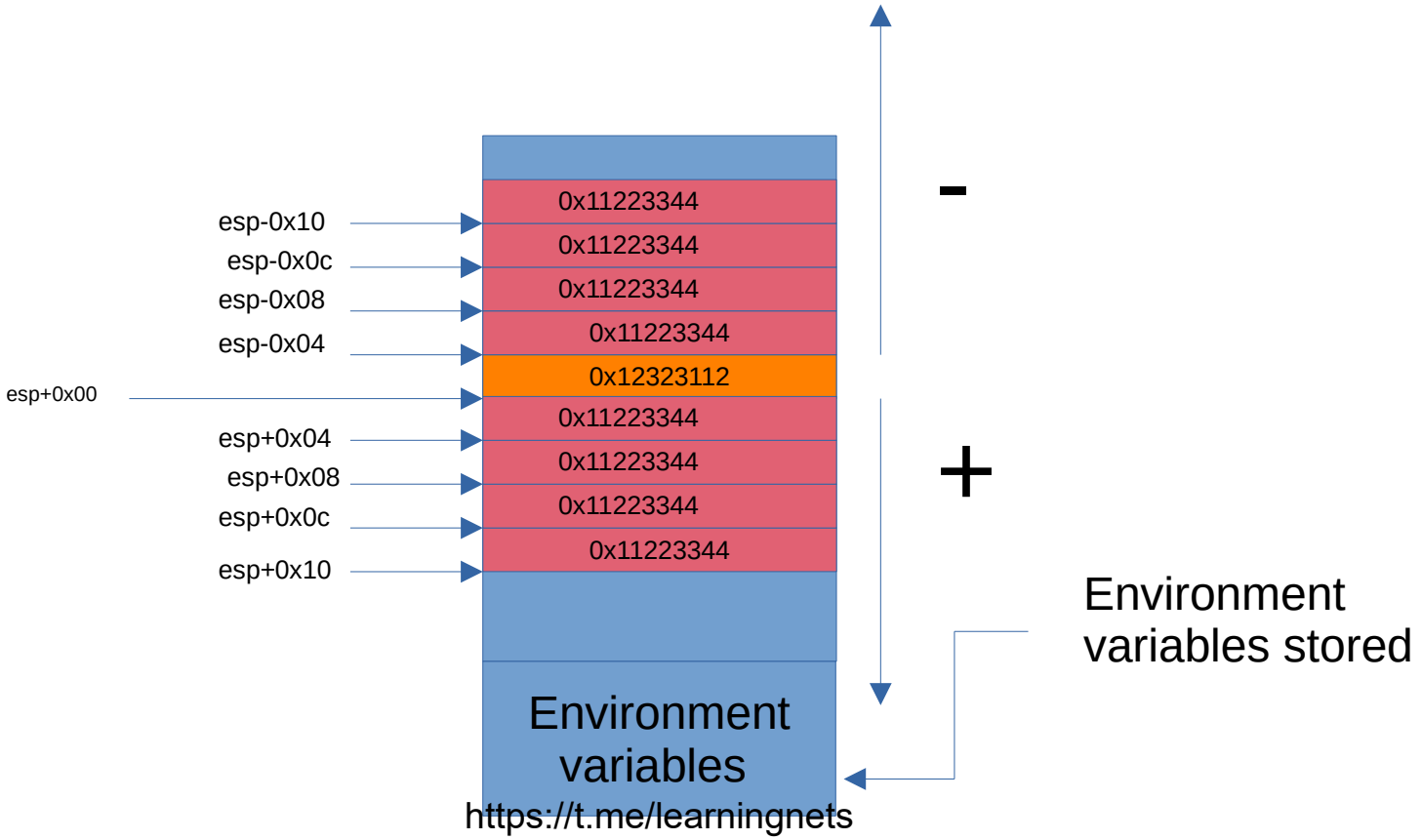
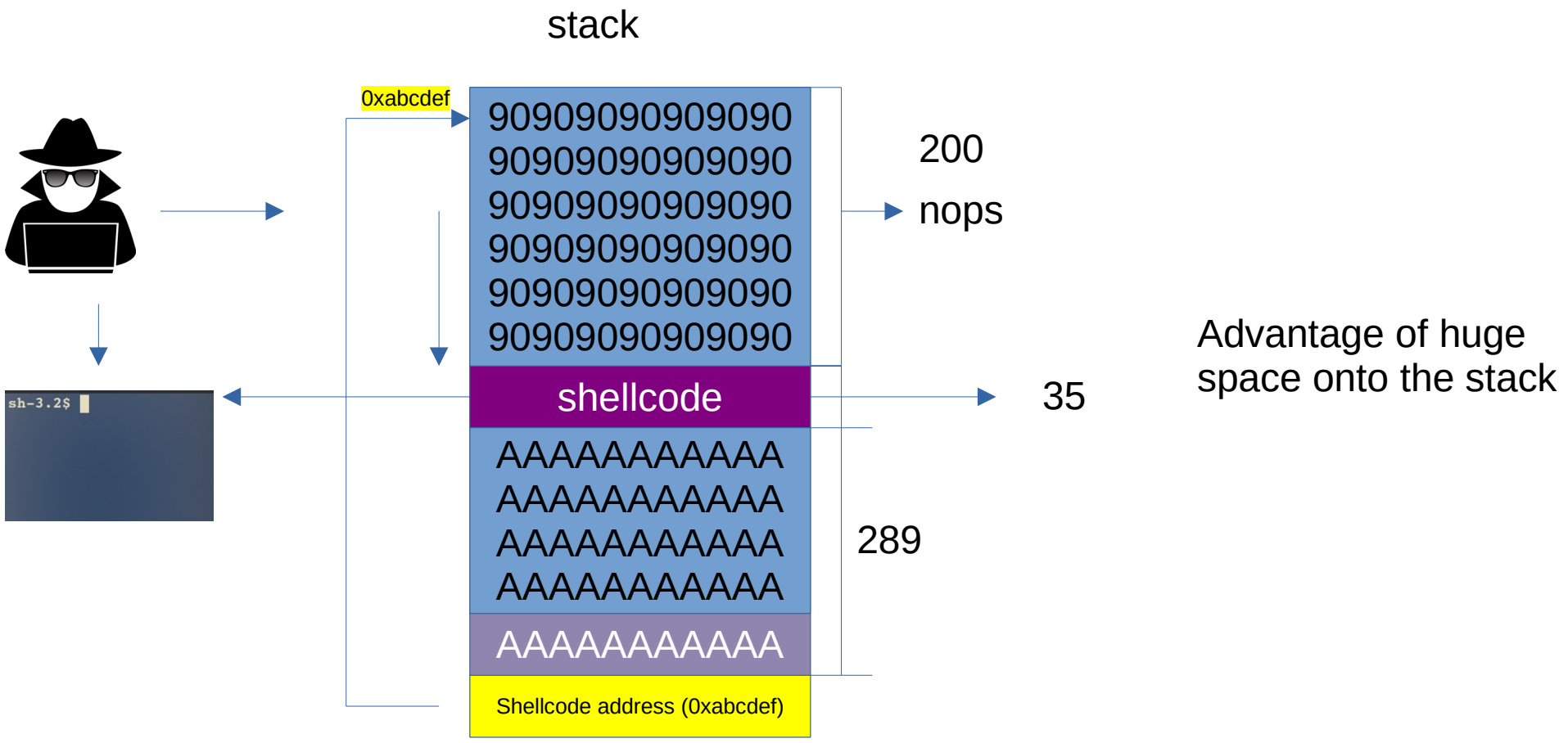
Stack up and down area

Environment variables on stack



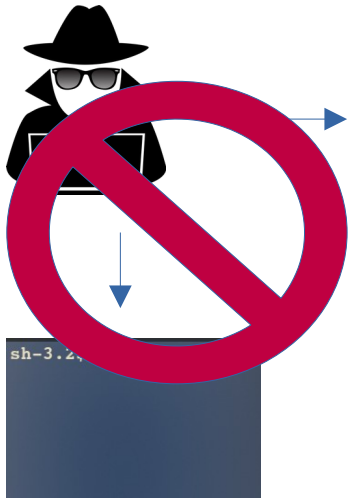
Total buffer = 524 (200+35+289)+jmp_address

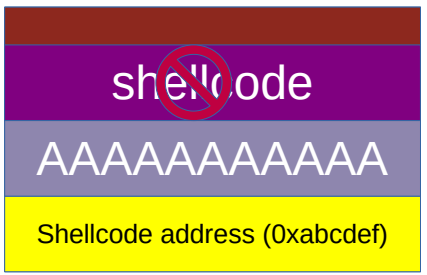


Advantage of huge space onto the stack

Total buffer = 524 (200+35+289)+jmp_address

stack

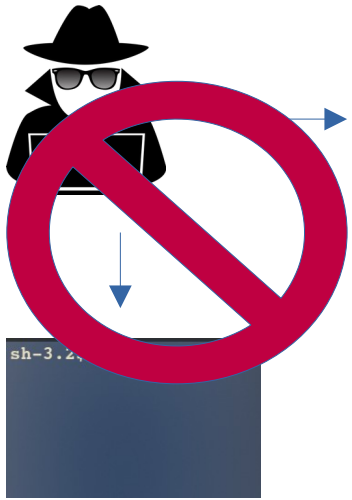


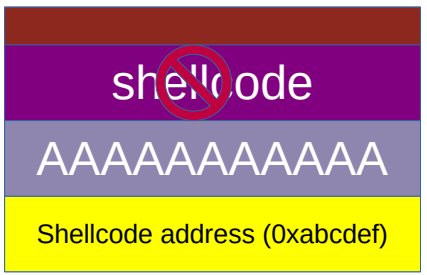


If there is shortage of space?

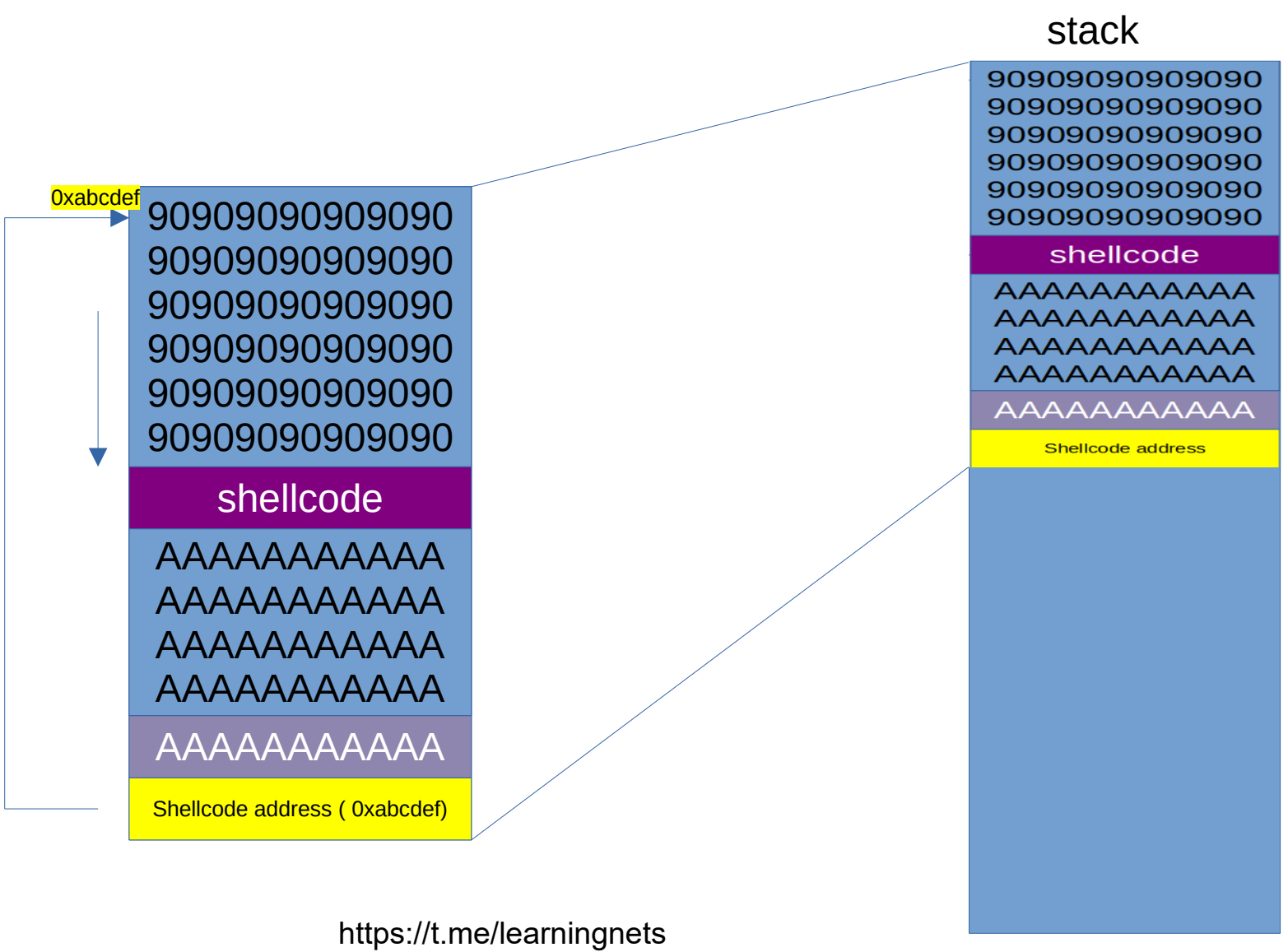
Total buffer = 524 (200+35+289)+jmp_address

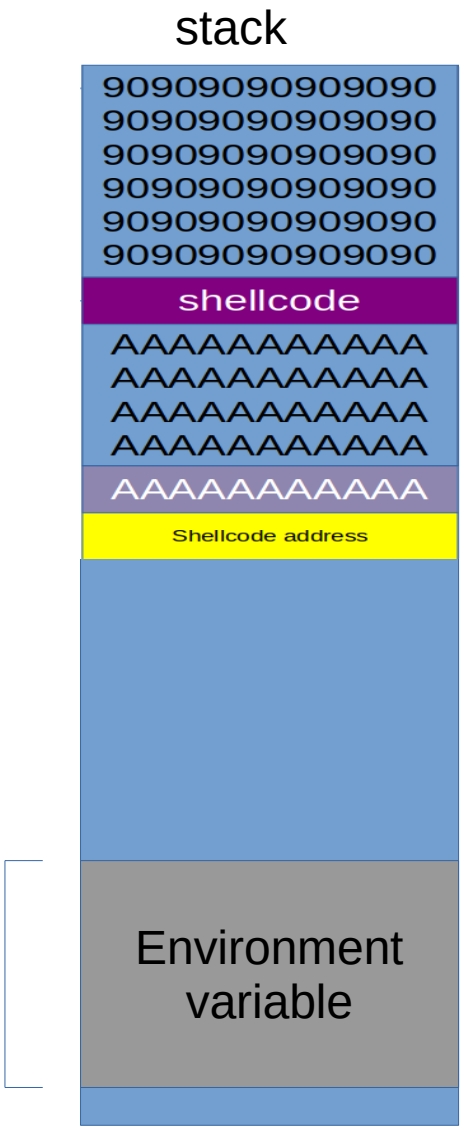
stack



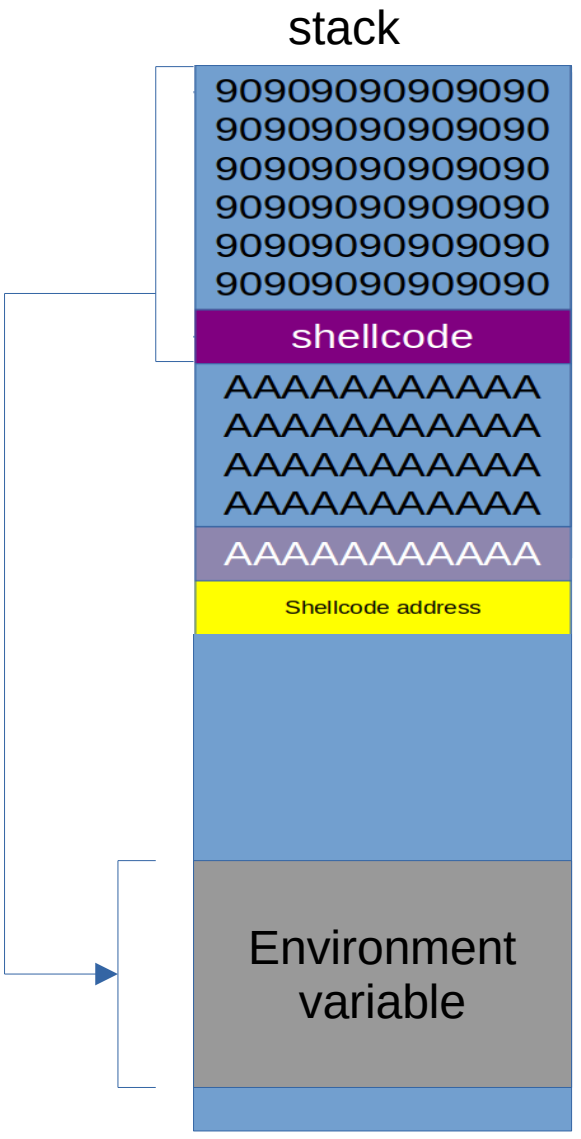


To overcome this situation we will use environment variable to store our shellcode inside the environment variable

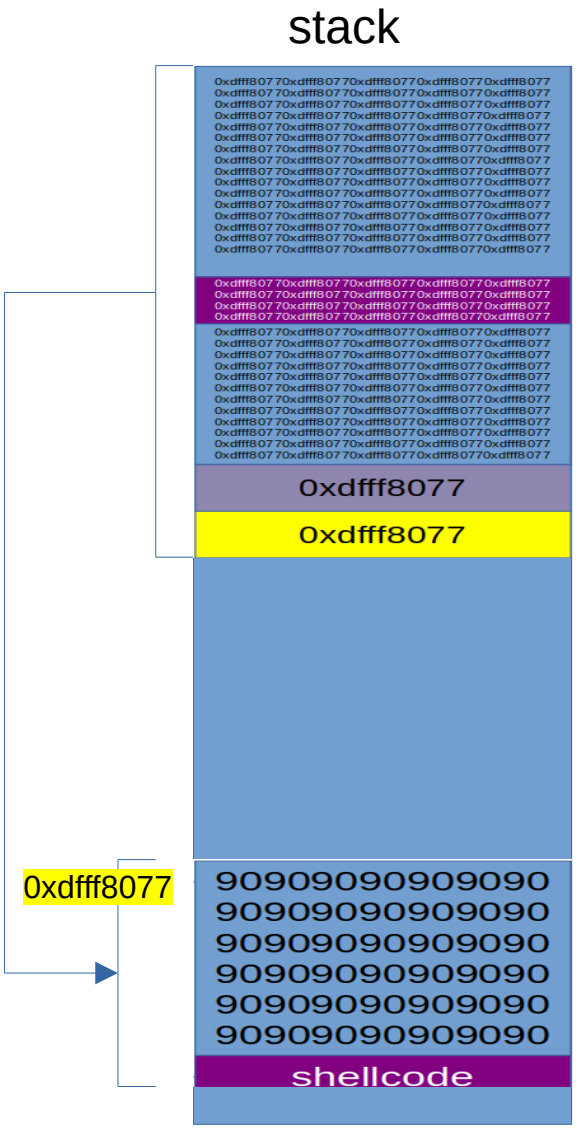


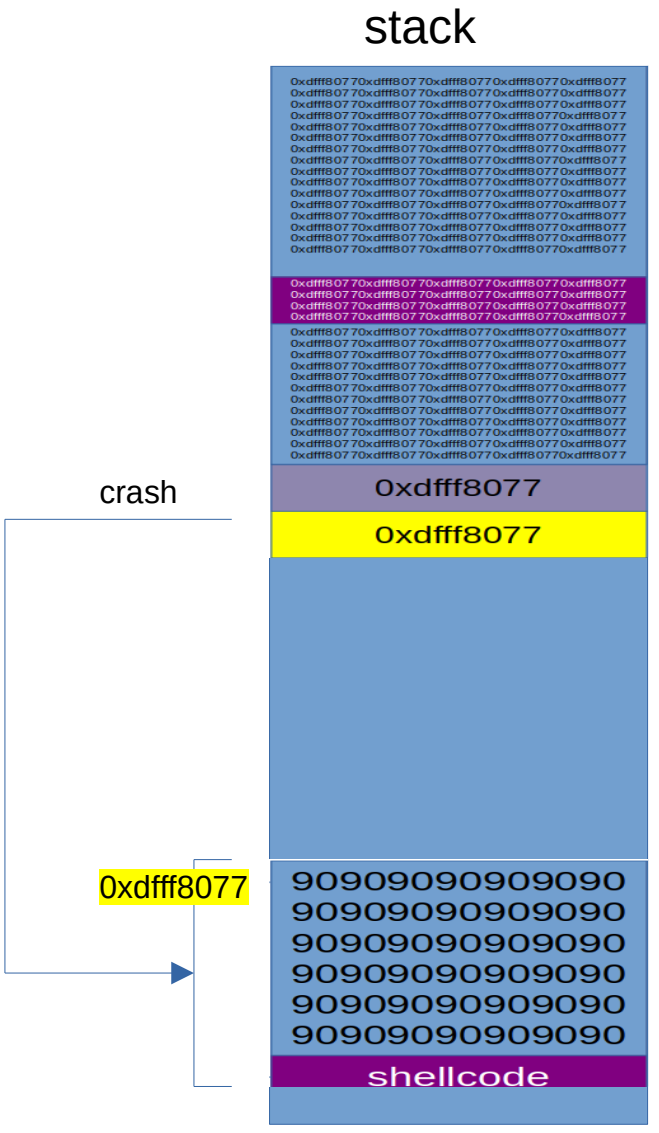


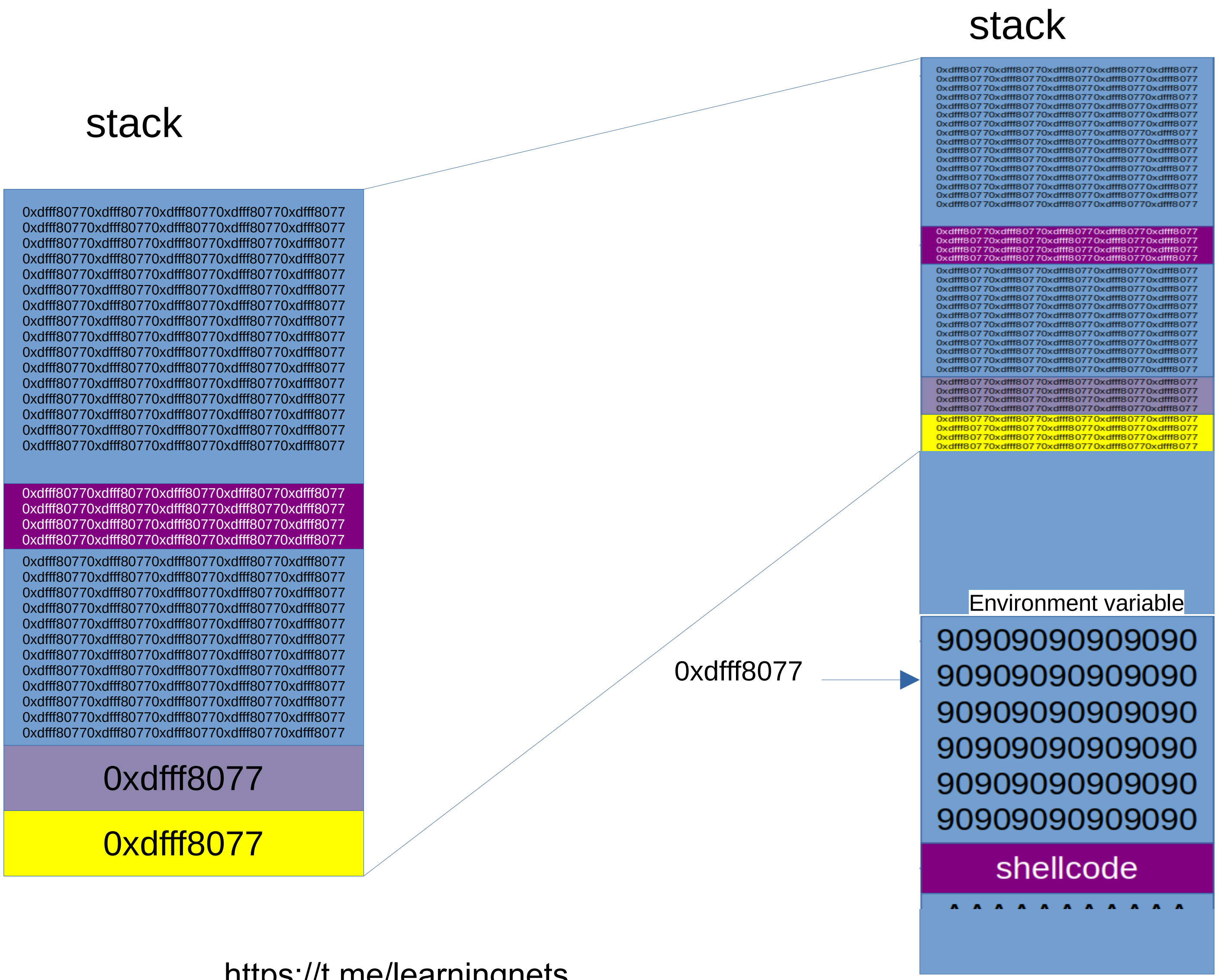
Saving our shellcode into environment variable



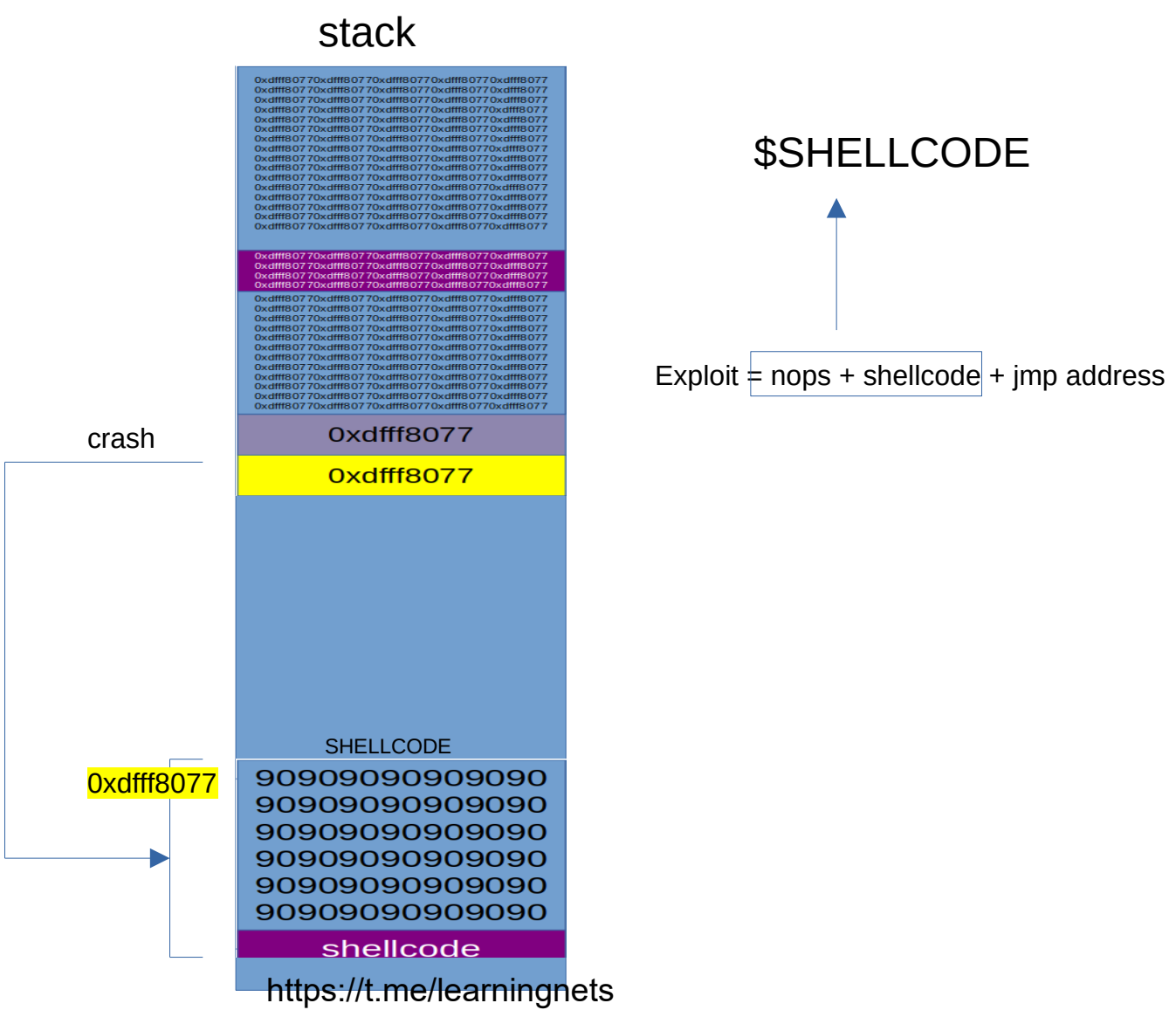
Filling the program input buffer with the address of our shellcode environment address onto the stack







https://t.me/learningnets


stack
$SHELLCODE
Exploit = nops + shellcode + jmp address
crash
0xdfff8077
0xdfff8077
SHELLCODE
0xdfff8077
9090909090909090909090909090909090909090909090909090909090909090
shellcode
https://t.me/learningnets