What is DEP(No eXecute bit)

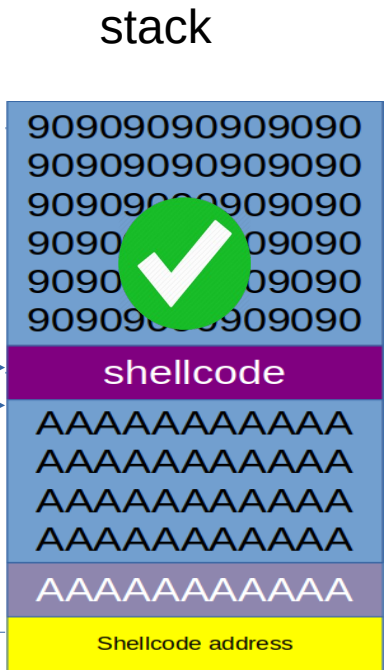
Data Execution Prevention – Data on the stack is not executable

By default this security option is enabled on compilation time of the binary

We can disable it by using -z execstack option in gcc

Without DEP protection

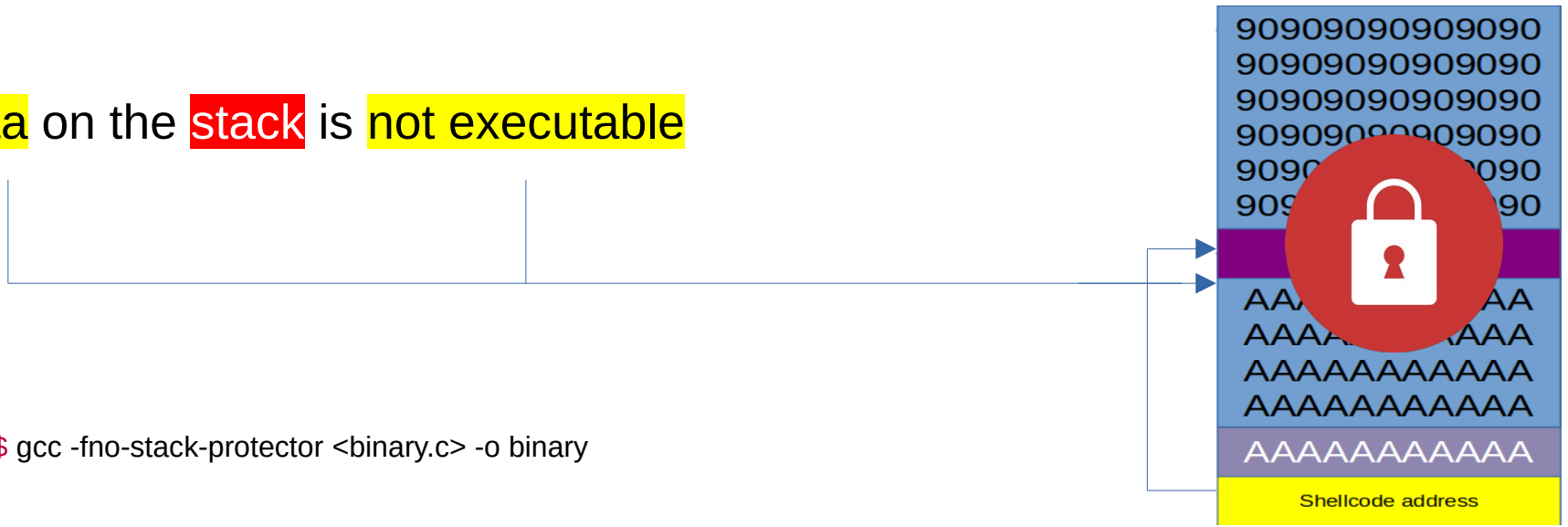
Data on the stack is executable



Linux$ gcc -z execstack -fno-stack-protector <binary.c> -o binary

With DEP (data execution prevention),No eXecute bit

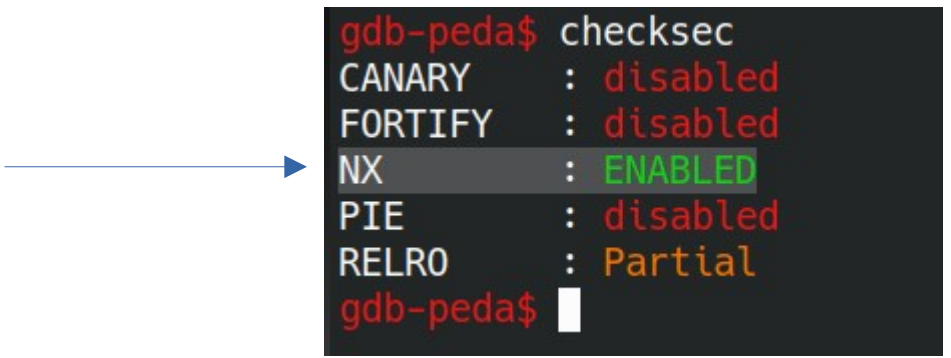
Data on the stack is not executable



Linux$ gcc -fno-stack-protector <binary.c> -o binary

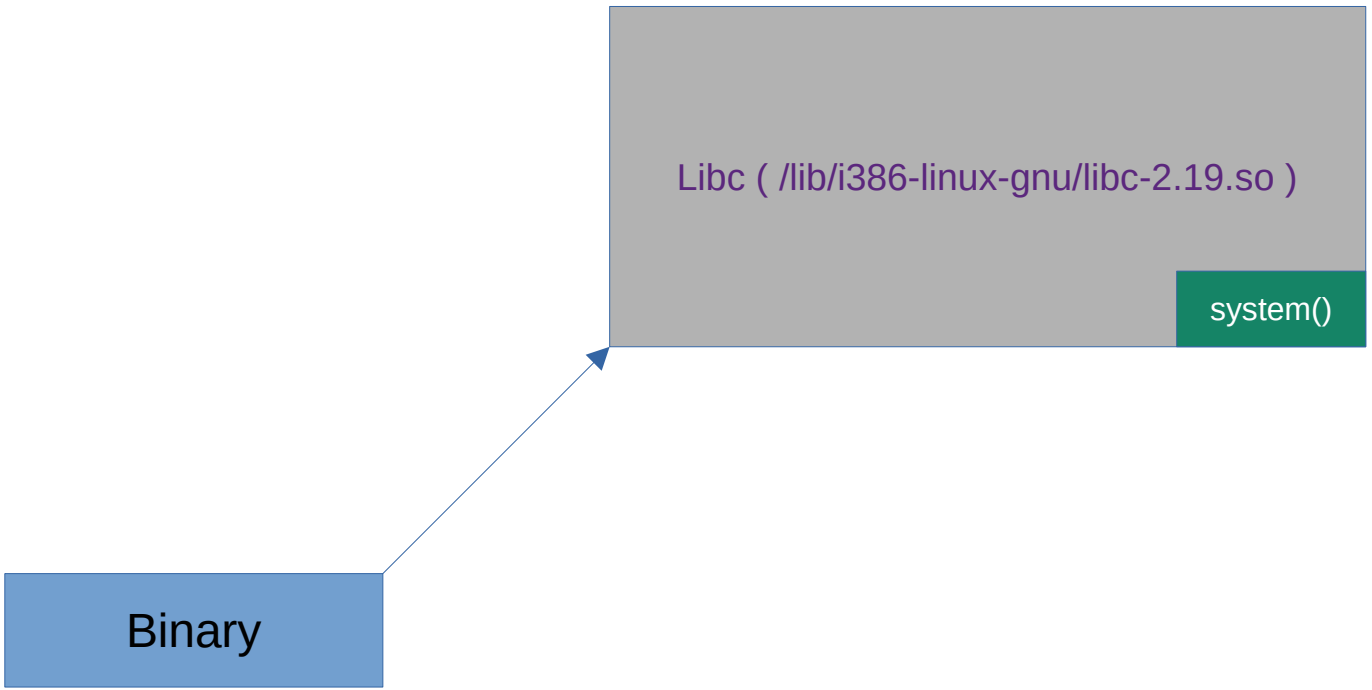
How to know if binary is DEP protected ?

gdb-peda plugin

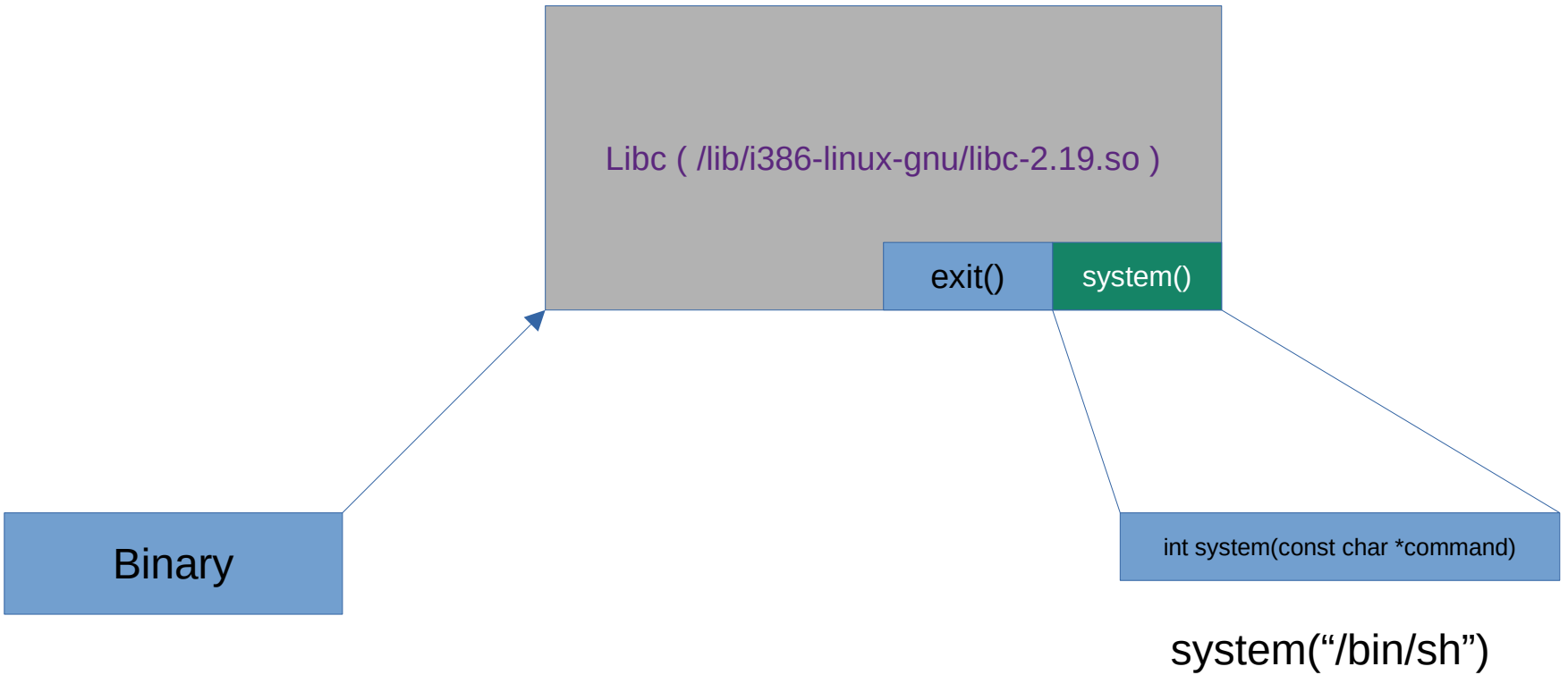


DEP enabled

Bypassing DEP

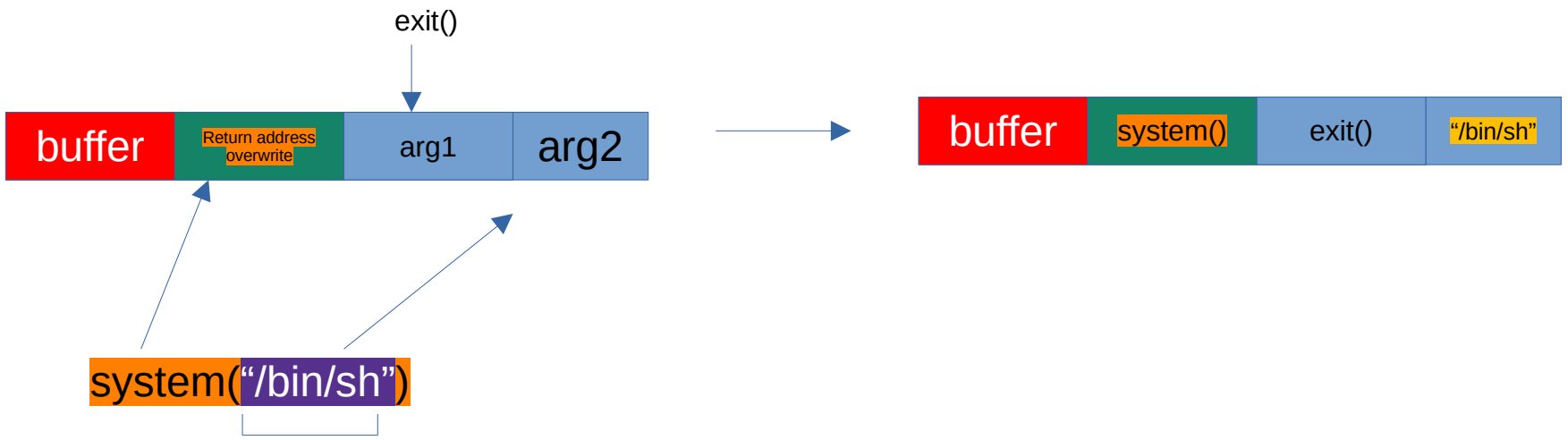


Bypassing DEP

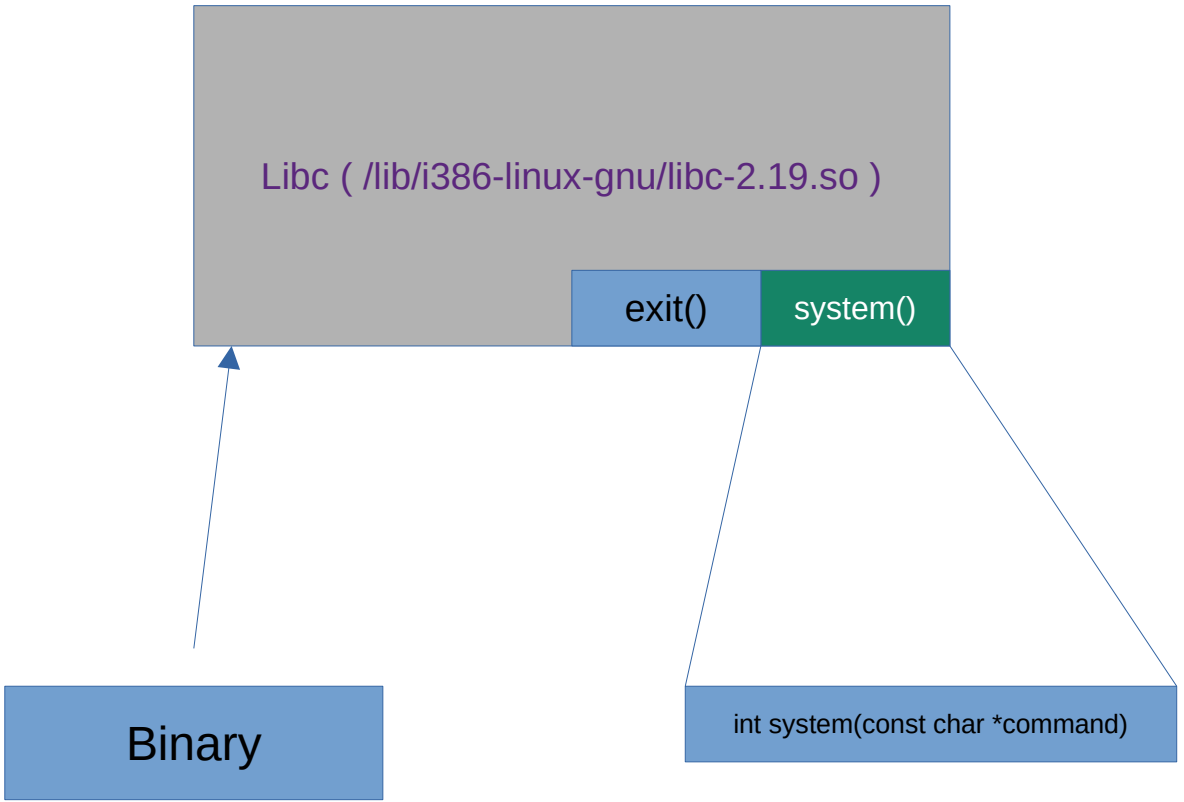


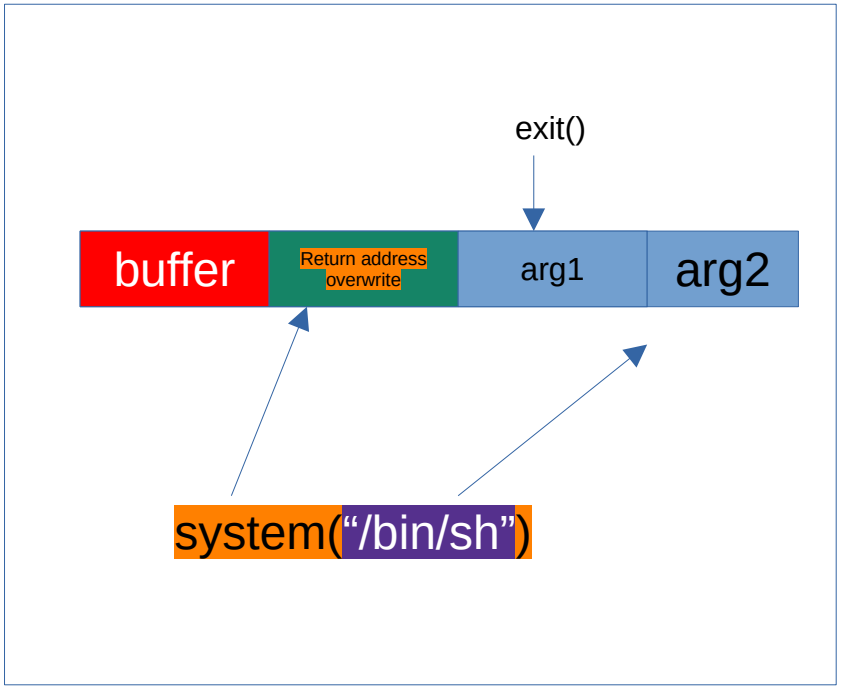
Bypassing DEP

exploit

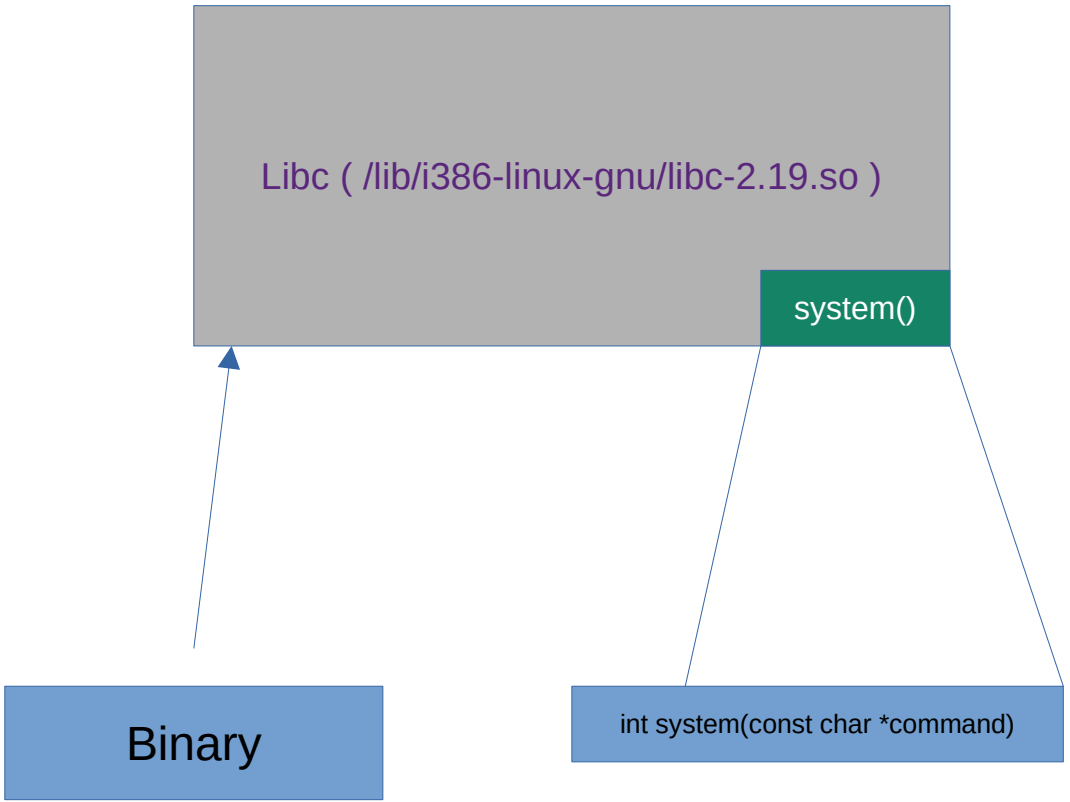


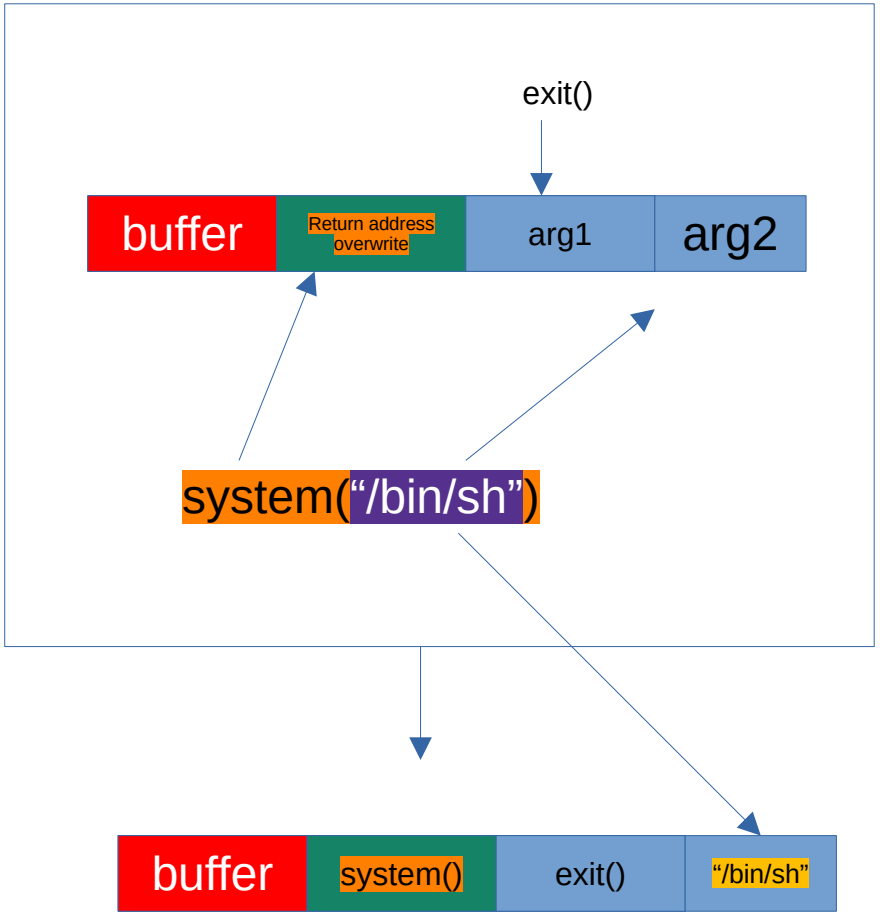
Bypassing DEP



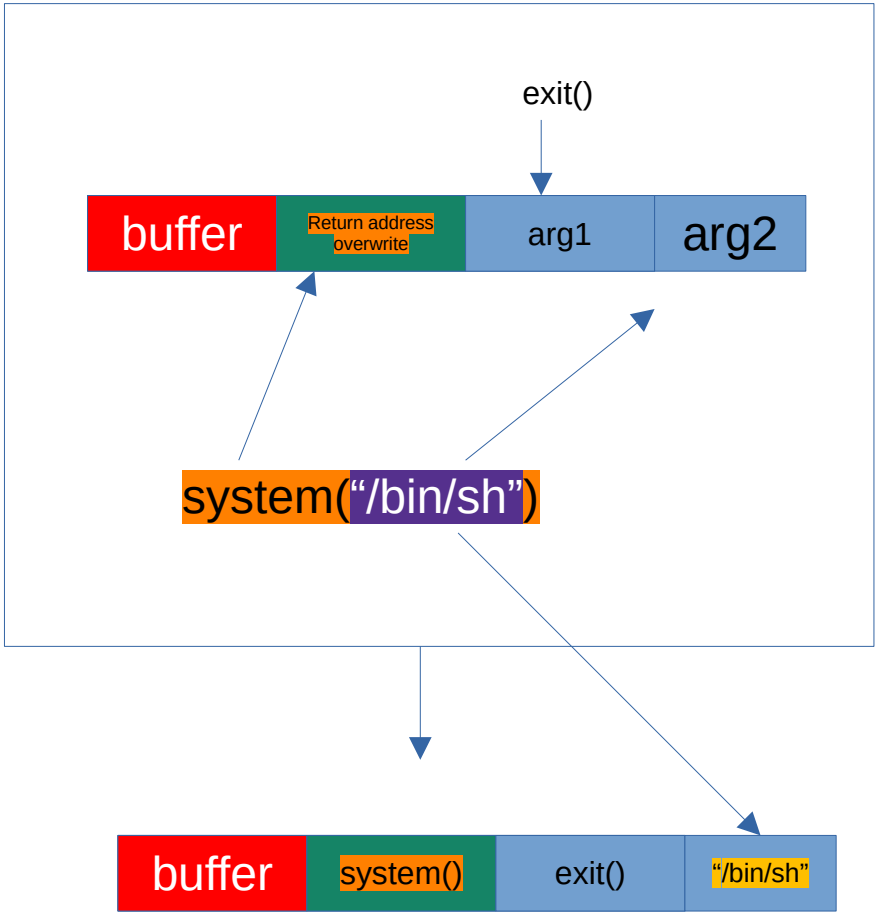


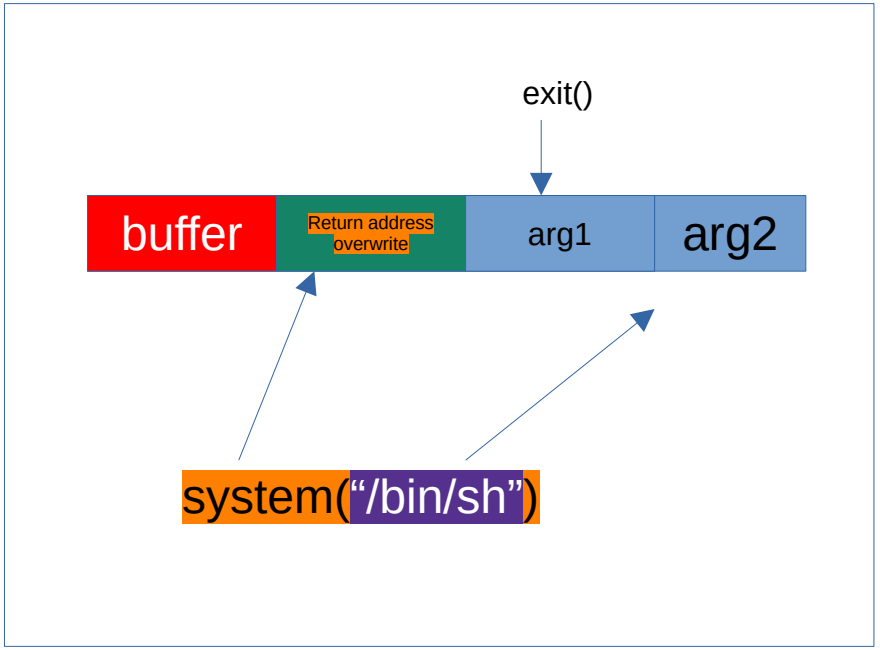
system(“/bin/sh”)

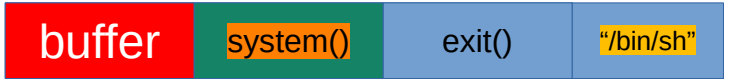




system("/bin/sh")







A*20 BBBB CCCC DDDD