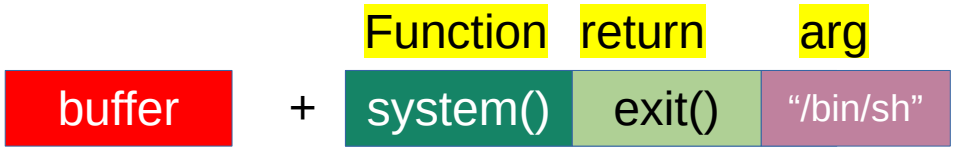
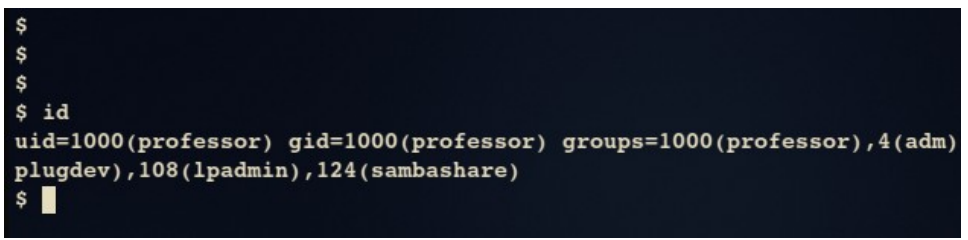
ROP exploits

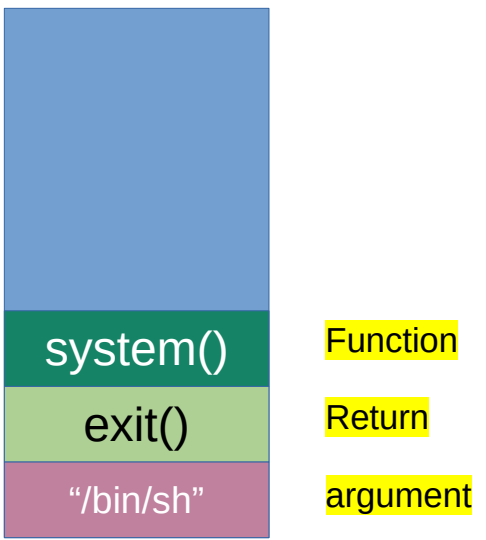
ROP stands for Return Oriented Programming

Return Oriented Programming (or ROP) is the idea of chaining together small snippets of assembly with stack control to cause the program to do more complex things.

How exploit works



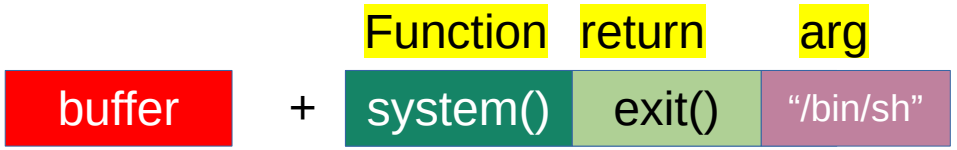




Stack cookie is disabled

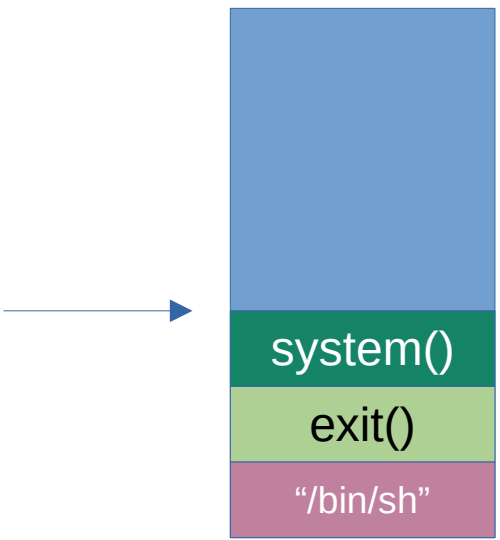
ASLR disabled

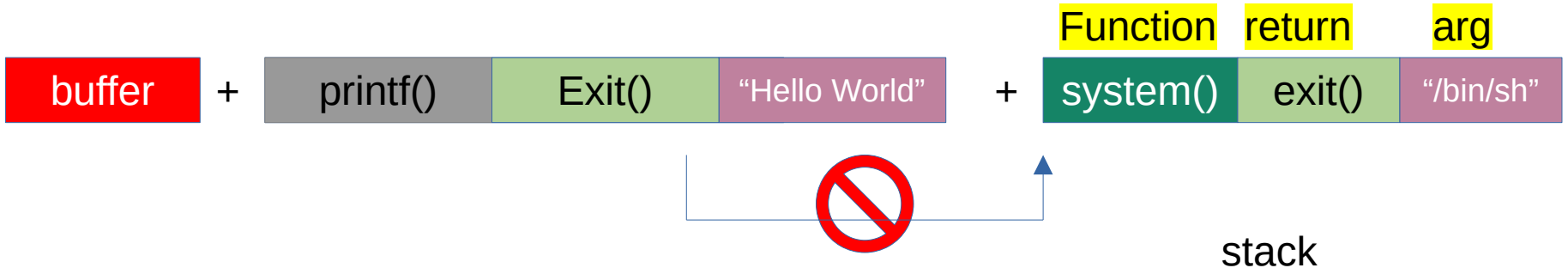
DEP Enabled



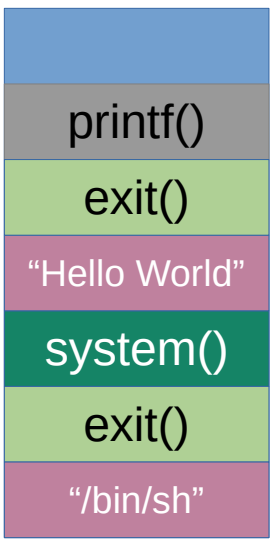
stack

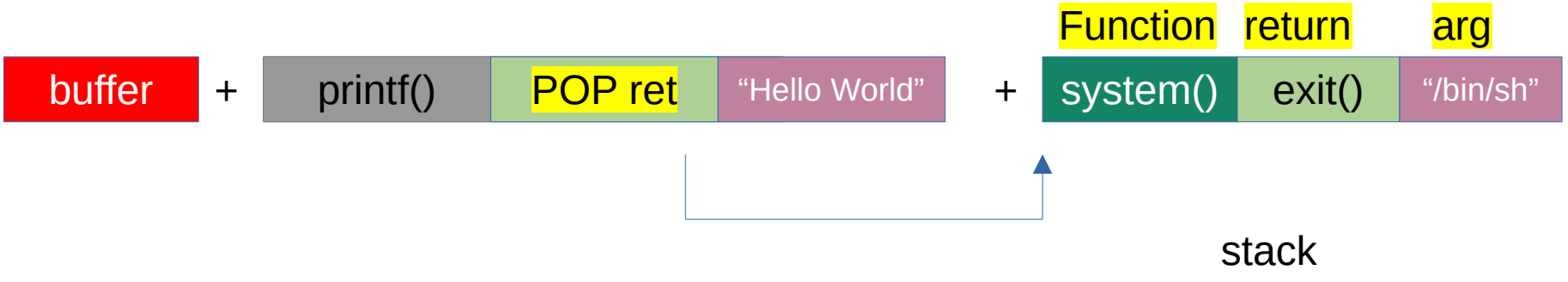
If we want to execute more funcitons on stack ?

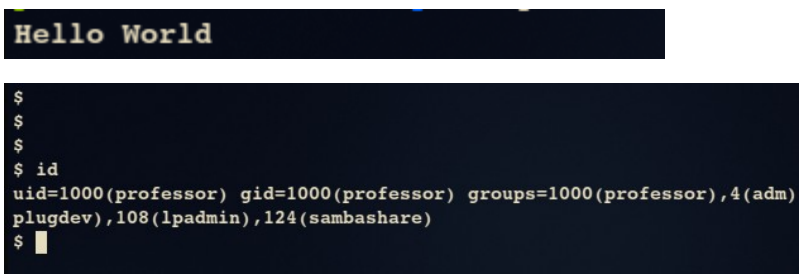


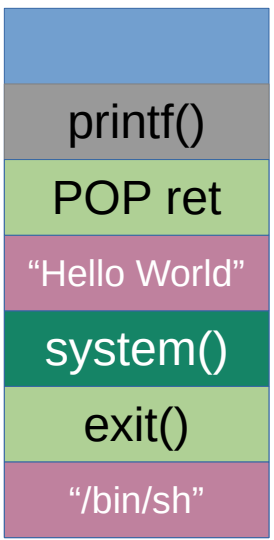


stack










```
Hello World
```

```
$
$
$
$ id
uid=1000(professor) gid=1000(professor) groups=1000(professor),4(adm)
plugdev),108(lpadmin),124(sambashare)
$
```