CSE 127

Week 3 Discussion

Zijie Zhao

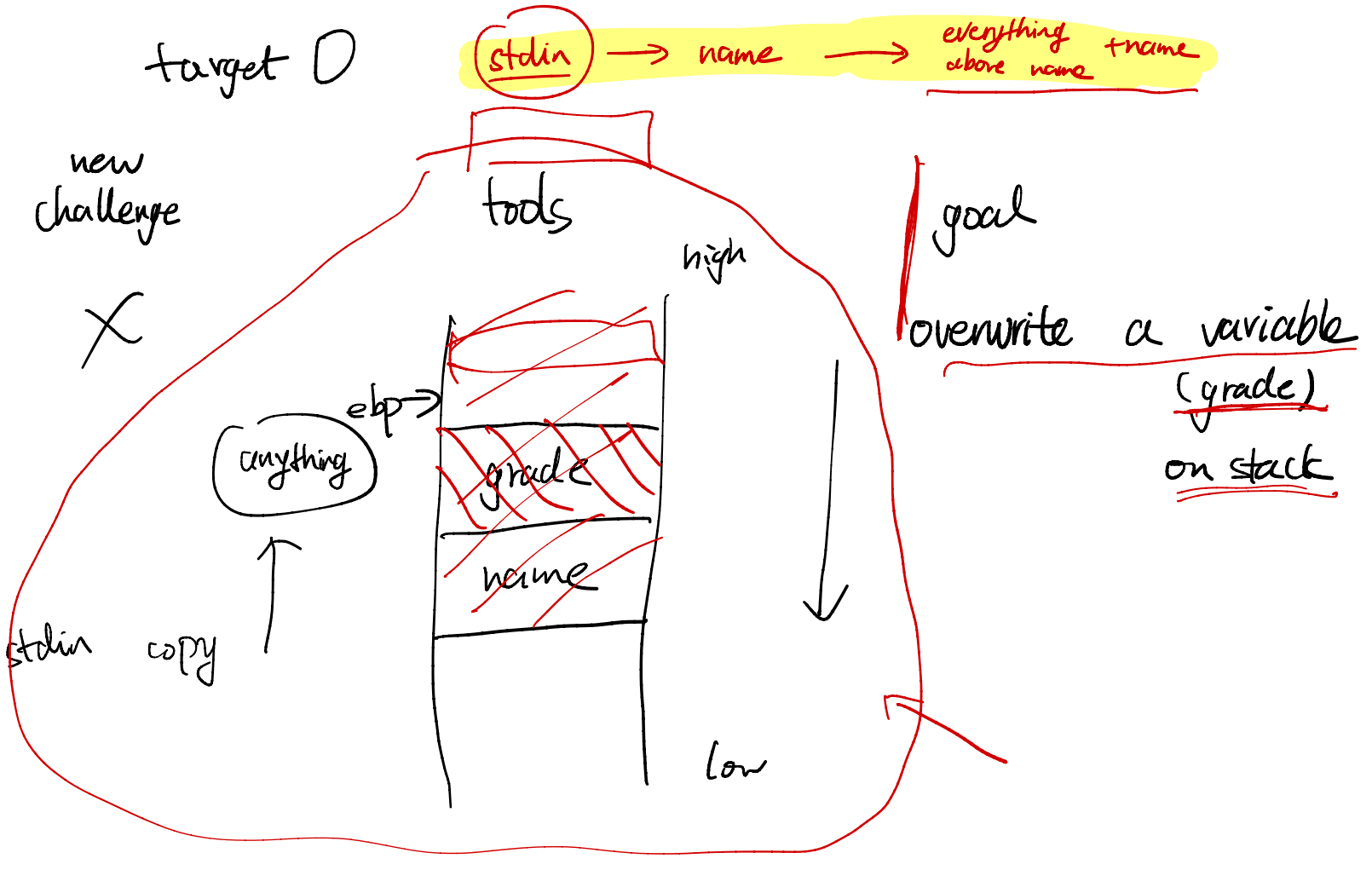
→ shell code < setuid
exec shell

→ gets vs. strcpy

'\n'

'0x00'

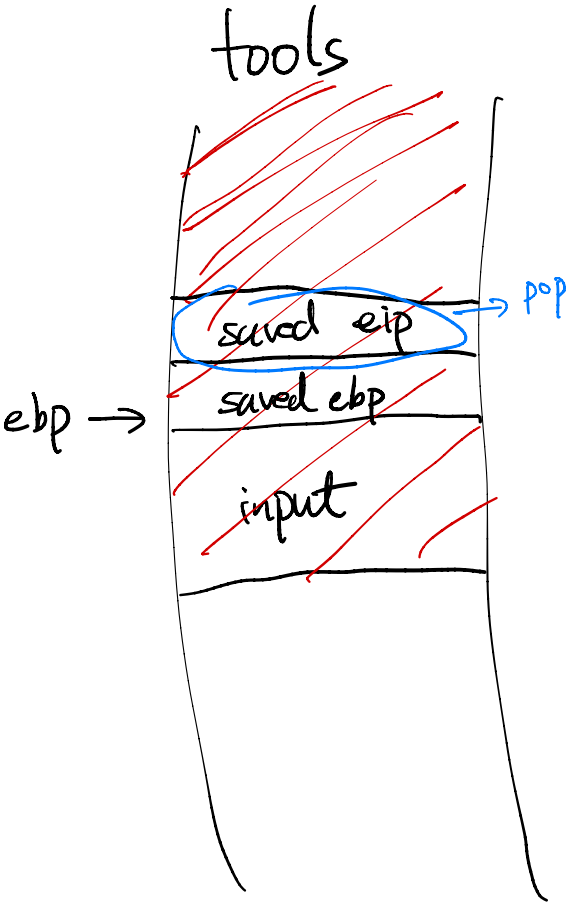
null


target 0
stdin
name
everything above name
tname
new challenge
X
tools
goal
overwrite a variable (grade) on stack
high
ebp
anything
grade
name
stdin
copy
low

target 1

challenge

X



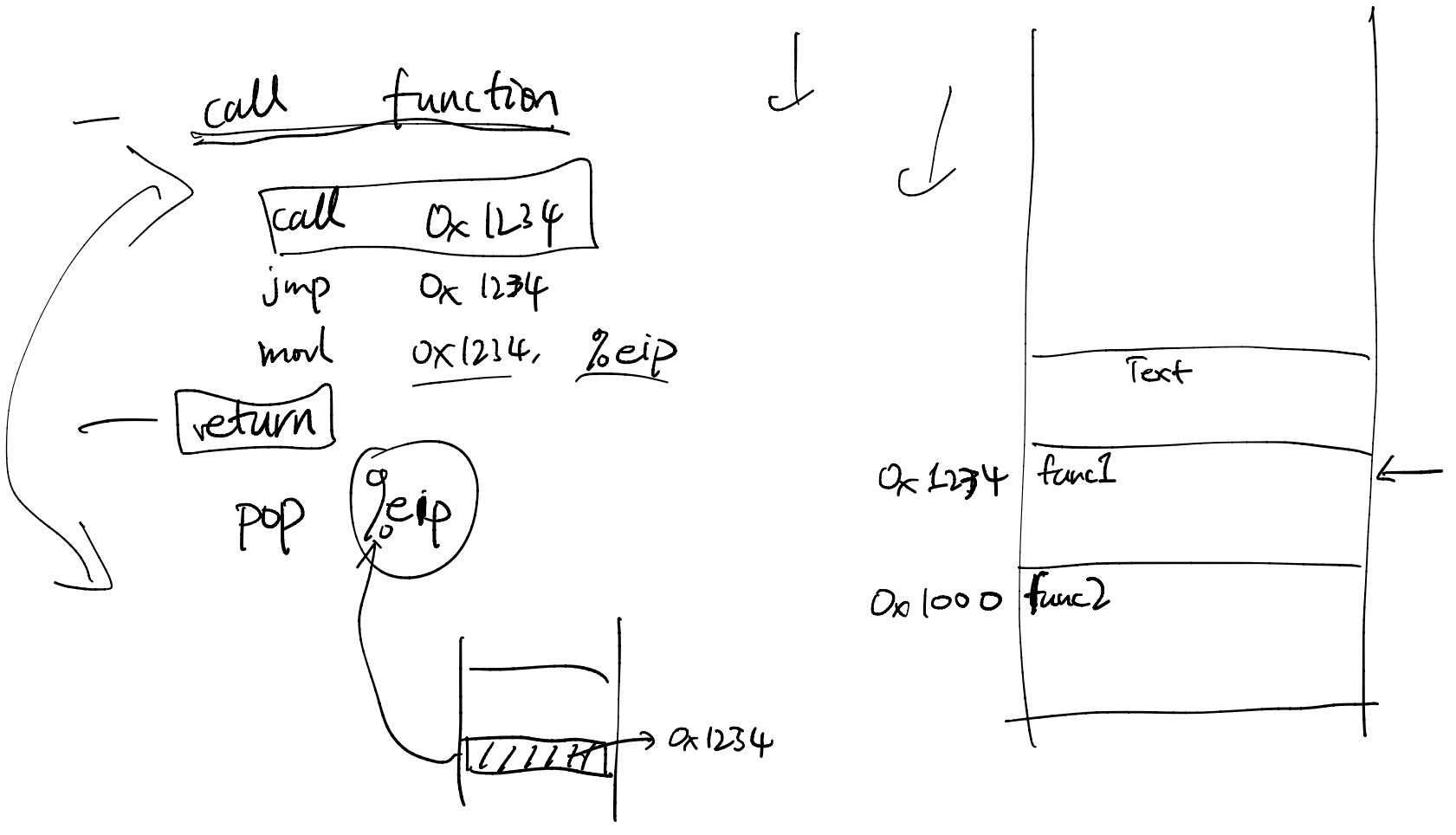
goals

overwrite

saved eip

to

print_good_grade

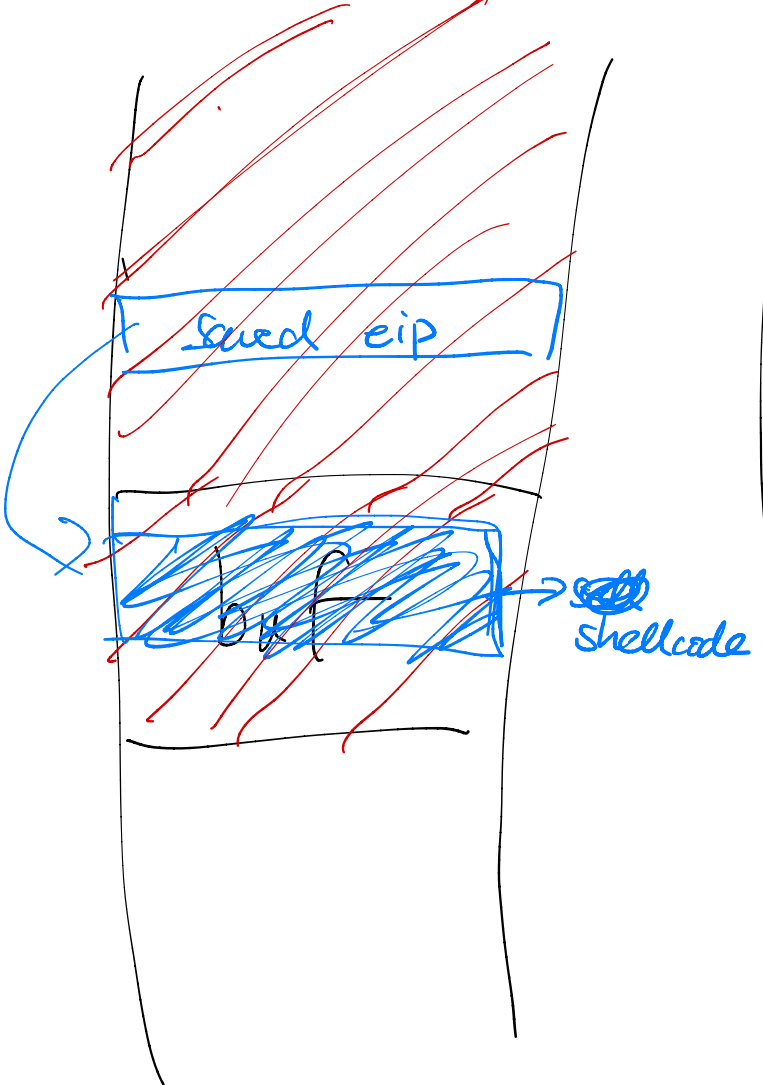

call function
call 0x1234
jmp 0x1234
movl 0x1234, %eip
return
pop %eip
0x1234
Text
0x1234 func1
0x1000 func2

target 2

challenge

strcpy

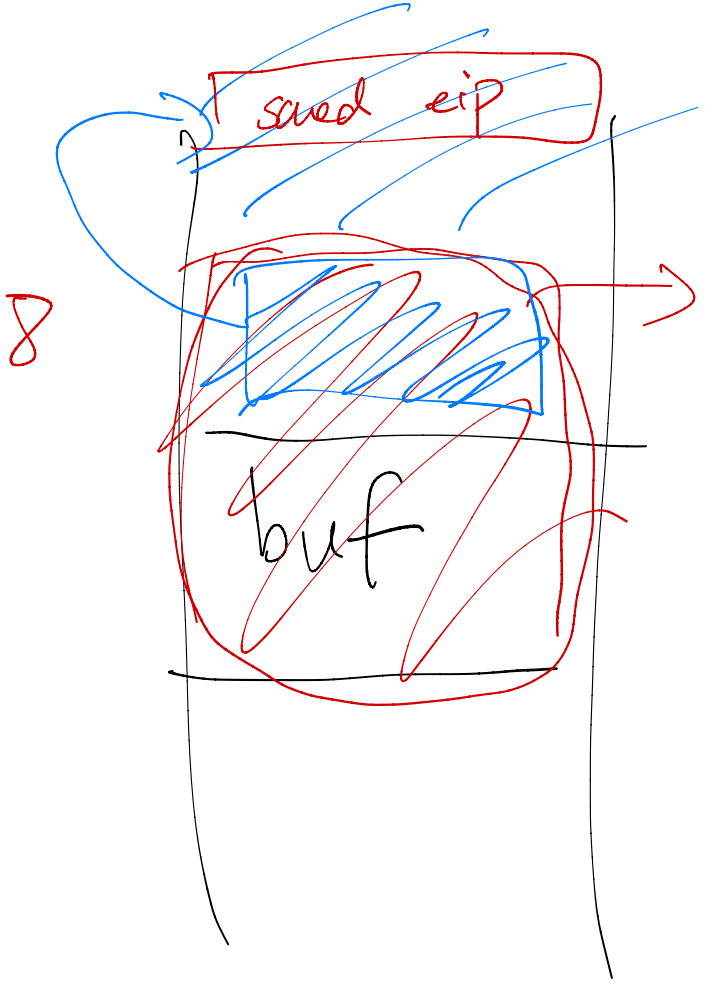
avoid null byte



goal

call shellcode

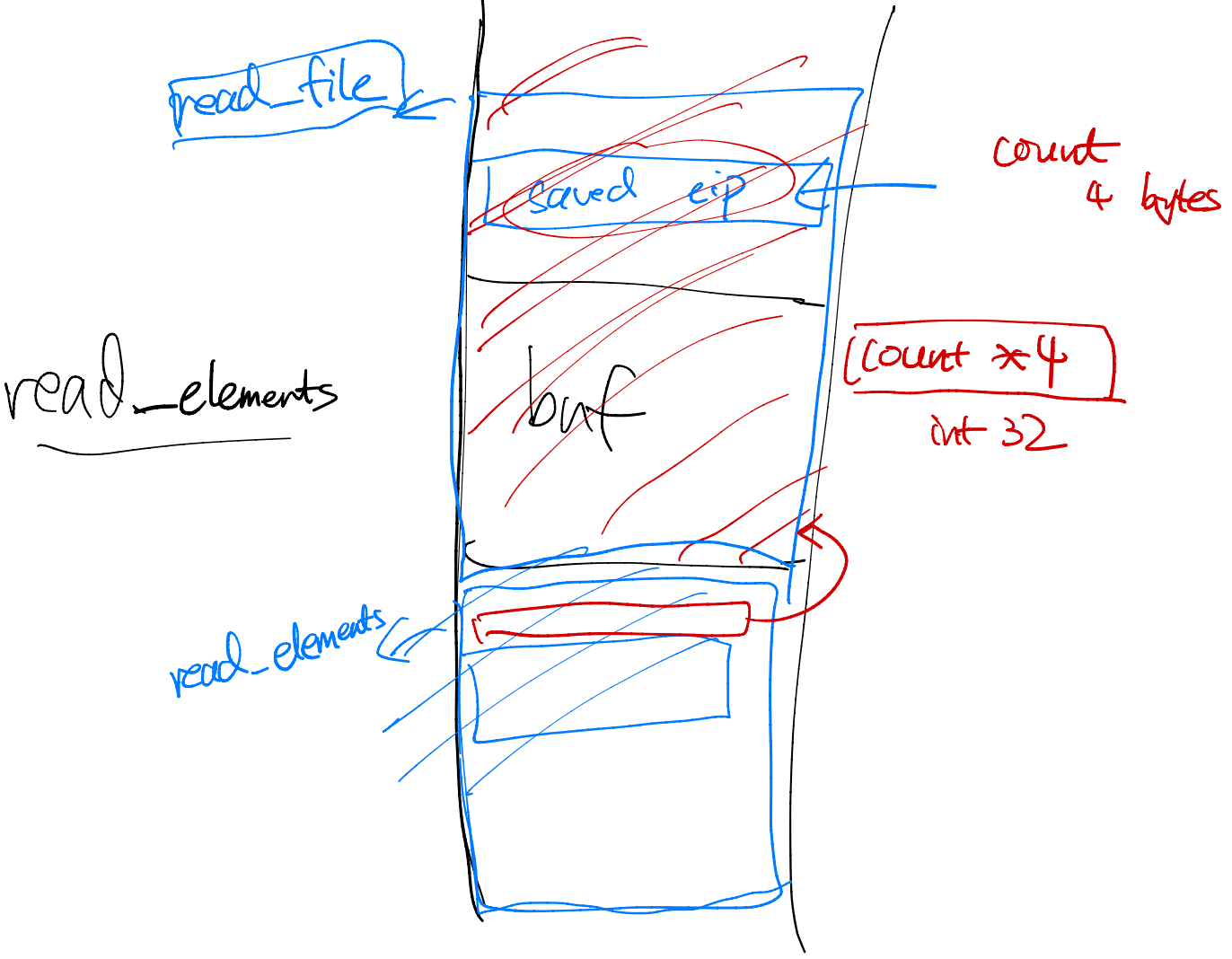
overwrite saved eip



8

goal

same


read_file
saved eip
count
4 bytes
read_elements
buf
count * 4
int 32
read_elements