Smashing the stack…

2016-06-09

Michael Denzel
m.denzel@cs.bham.ac.uk

“Tell Me and I Will Forget;
Show Me and I May Remember;
Involve Me and I Will Understand.“

- Confucius

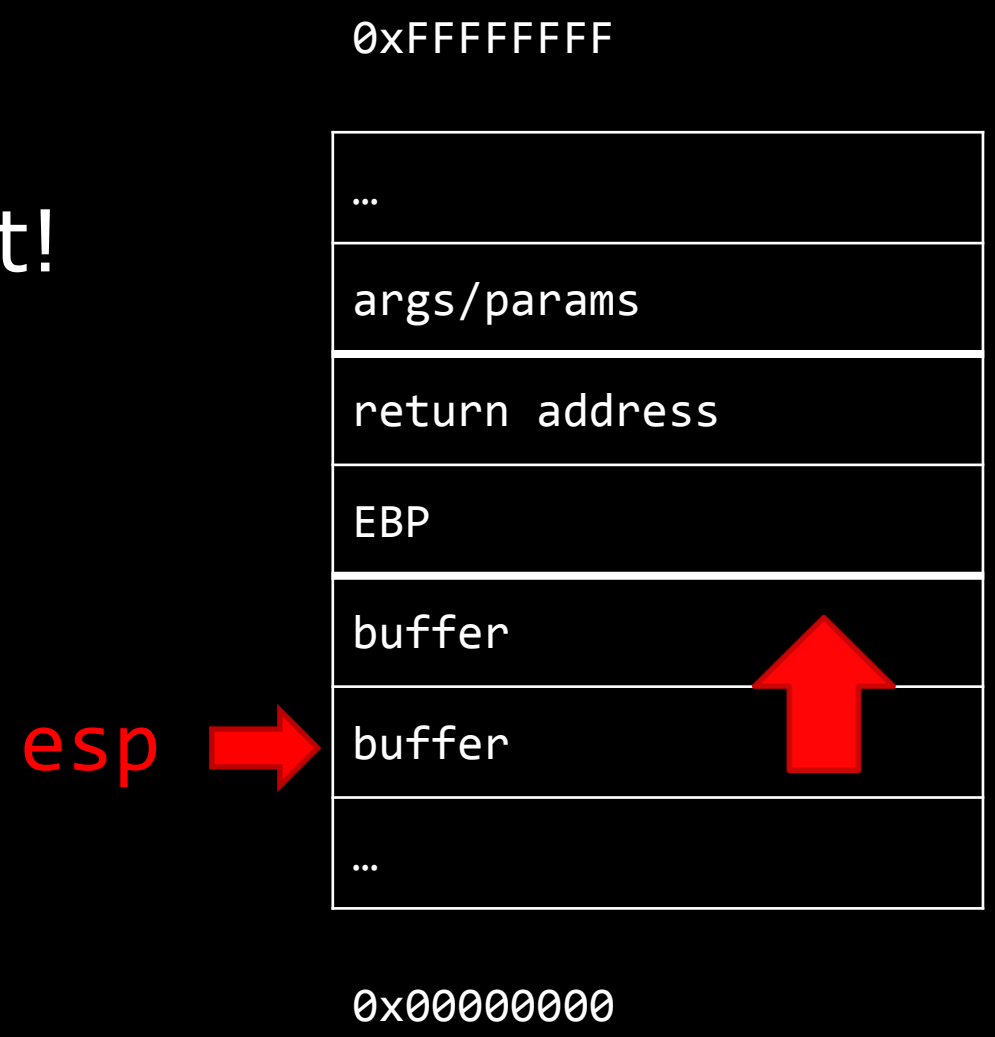
Download!

https://exploit-exercises.com/

“Protostar Exercise”

Buffer Overflow

- Stack alignment!
- Endianess!
- (ASLR)
- (NX bit)



Happy Hacking!

- start bash!
- objdump –d <file> | less
- gdb
  - b main
  - run < input
  - layout asm
  - si
  - ni
  - info frame → eip
  - x/2x $ebp → ebp
  - x/20x $esp → stack
- python –c “print ‘A’*1337 + ‘\x08’”
- Level 5: http://shell-storm.org/shellcode