CS 208

Mon, 27 Feb 2023
getbuf:
  sub N, %rsp
  call <gets>
  add N, %rsp
  ret8

```
N
{}
```

ret addr to test
addr of touch!

ret8

1. Grab 8-byte address
   rsp is pointing to
2. Jmp there
3. Add 8 to rsp
by evil instructions here

addr of instructions

Useful technique

One step

0. Push target address

1. Push target instructions in evil
all the bad code
(and sub 0x1000, %esp)

fatadir