The Friday TA Crew Presents…
Buffer Part III
What are we trying to achieve?
What are we trying to achieve?
We want to overwrite this
We want to overwrite this with the address of this.
We want to overwrite this
with the address of this
so we can run this code
We want to overwrite this with the address of this so we can run this code.
So what tools do we have to achieve this?
GDB
Useful GDB Tools:

- **x [address]**
  - Try running `x $rsp` to find the address of rsp!
  - `x/[number] $rsp` (i.e. `x/64 $rsp`).
- **info reg**
  - get the information of the registers
- **disass**
  - disassembles
- **si**
  - step instruction
- **info proc mapping**
  - gives you a mapping of the memory