

CS 208

F, 20 Feb 2026

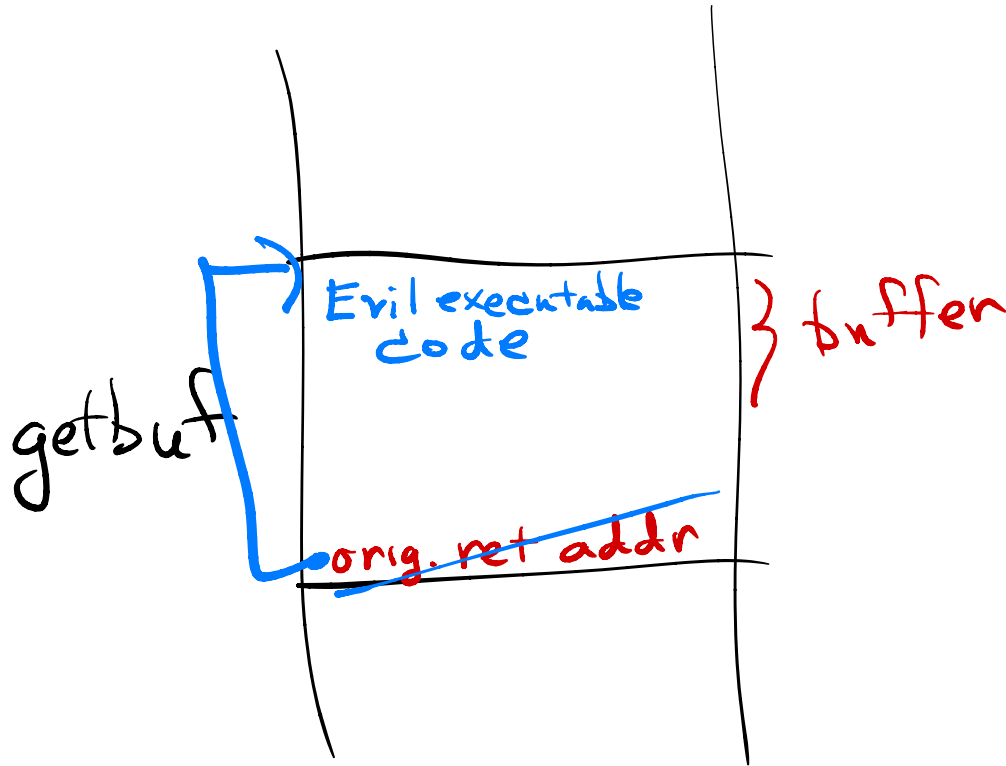
Phase 1



goal get
your input (being
read by GetS
into buffer)
to overwrite
return address

Phase 2

Advice



Advice

1. Don't skip Appendix B

```
gcc -c .....  
objdump -d .....
```

2. In your evil code, don't use `call`; use `ret`

(push addr of where you want to go, then `ret`)