foo()
{
    char buf[80];
    char *p = buf;
    while (((p++) = getchar()) != '\n')
        ;
    . . .
}

C code

caller's stack frame

return addr from foo()

exploit code

return to exploit code

char buf[80]

stack before exploit

stack after exploit

increasing memory addresses

increasing memory addresses

char *p