

## File: myls.s

```
section .text
global _start
_start:
    ; store the arguments on stack
    xor    eax, eax
    push   eax                ; use 0 to terminate the string
    push   "-la "
    push   "ls  "
    push   eax                ; use 0 to terminate the string
    push   "-ccc"
    push   eax                ; use 0 to terminate the string
    push   "//sh"
    push   "/bin"
    mov    ebx, esp           ; ebx = address of command "/bin//sh"

    ; setup argument array argv[] on stack
    push   eax                ; argv[3] = 0
    mov    eax, ebx           ; argv[2] = address of "ls -la"
    add    eax, 20
    push   eax
    mov    eax, ebx           ; argv[1] = address of "-ccc"
    add    eax, 12
    push   eax
    push   ebx                ; argv[0] = address of "/bin//sh"
    mov    ecx, esp           ; ecx = address of argv[]

    ; no environment variables to pass to execve()
    xor    edx, edx           ; edx = 0x00000000

    ; invoke execve()
    xor    eax, eax           ; eax = 0x00000000
    mov    al, 0x0b           ; eax = 0x0000000b
    int    0x80
```

Setup for `execve ( )` to execute the command: `/bin/sh -c "ls -la"`

