SHELLCODE

ShellCode

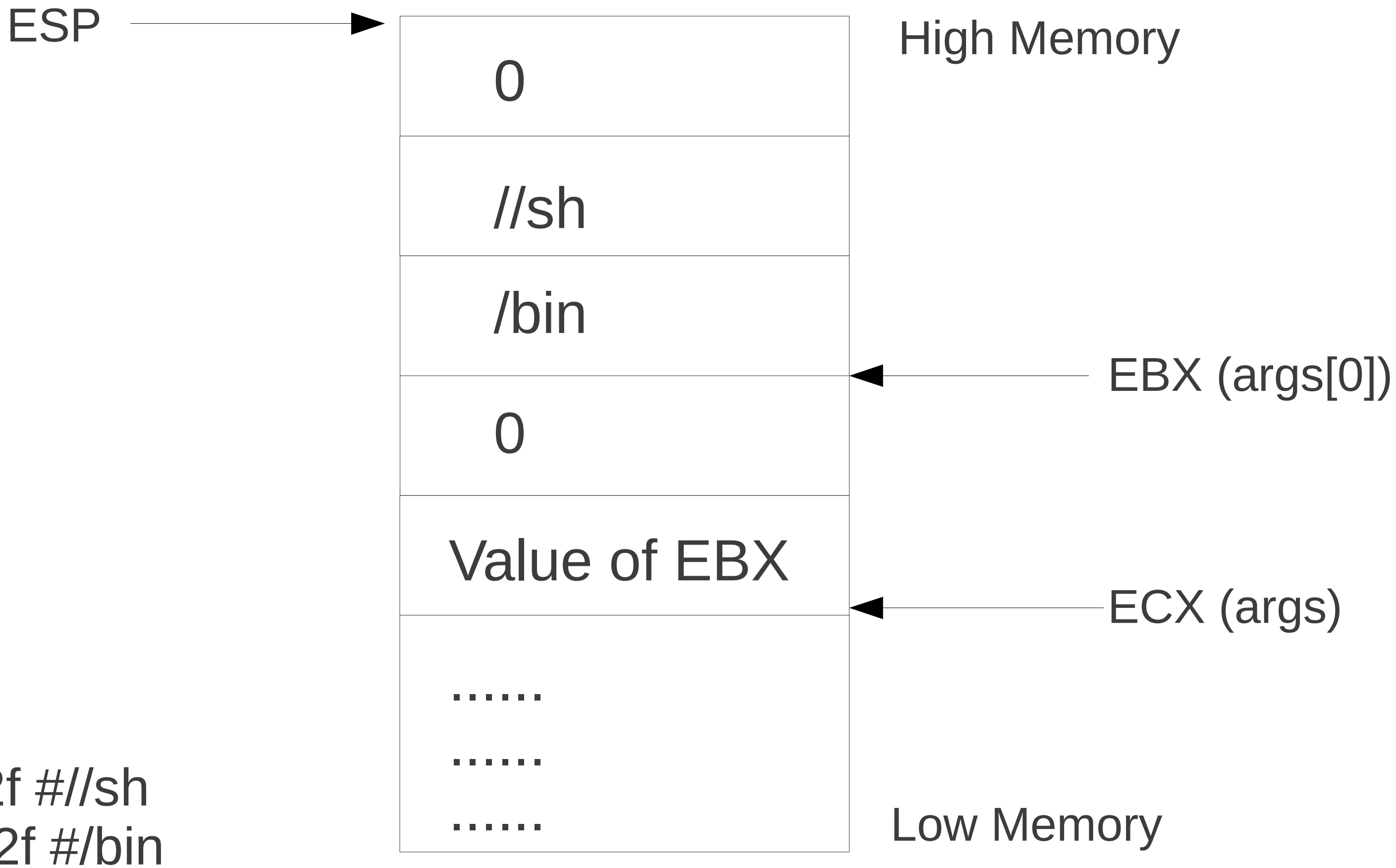
- Machine code with specific purpose

  - spawn a local shell

  - create a new account
- Executed directly by CPU

  – no assembling / linking or separate compiling required
- Shellcode should be small and free of NULL bytes

Stack



ESP

High Memory

0

//sh

/bin

EBX (args[0])

0

Value of EBX

ECX (args)

......

......

......

Low Memory

```
xor  %eax,%eax
push   %eax
push   $0x68732f2f #//sh
push   $0x6e69622f #/bin
mov    %esp,%ebx
push   %eax
push   %ebx
mov   %esp,%ecx
xor     %edx,edx
mov    $0xb,%al
int    $0x80
```

```
//C code Snippet

args[0] = "/bin/sh";
args[1] = NULL;
execve(args[0], args, NULL); //(ebx,ecx,edx)
```

Commands

- Objdump

  - objdump -d <binary>

- Compiling with disabling stack protection

  - gcc -fno-stack-protector -z execstack <file.c>

Task

Write a shell code to enable write operation(chmod 666) for all users to /etc/shadow