ShellCode

- First create hello.asm file using text editor

```
section .data
        text db "Hello World!!",10

section .text
        global _start

_start:
        mov rax, 1
        mov rdi, 1
        mov rsi, text
        mov rdx, 14
        syscall

        mov rax, 60
        mov rdi, 0
        syscall
```

- Then compile it using following commands

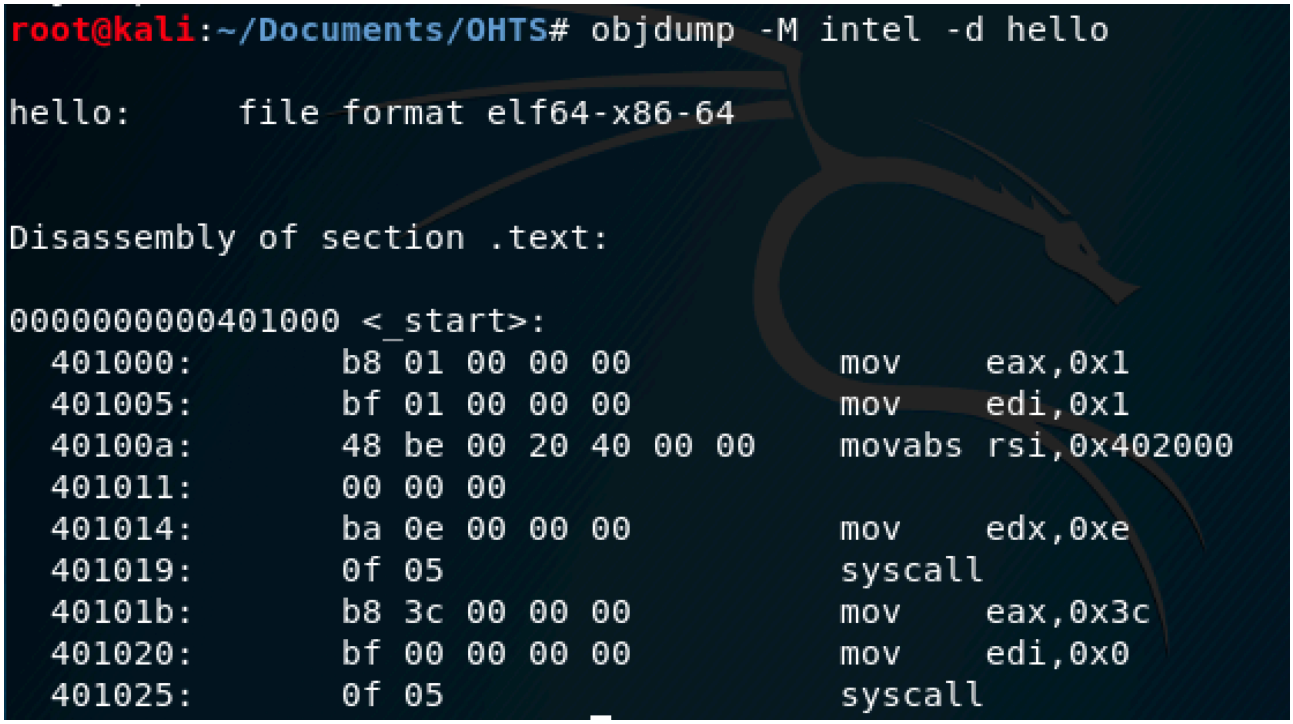
```
root@kali:~/Documents/OHTS# nasm -f elf64 -o hello.o hello.asm
```

```
root@kali:~/Documents/OHTS# ld hello.o -o hello
```

- Then run it

```
root@kali:~/Documents/OHTS# ./hello
Hello World!!
```

- Then extract the shellCode



- ShellCode :

“\xb8\x01\x00\x00\x00\xbf\x01\x00\x00\x00\x48\xbe\x00\x20\x40\x00\x00\x00\x00\x00\xba\x0e\x00\x00\x00\x0f\x05\xb8\x3c\x00\x00\x00\xbf\x00\x00\x00\x00\x0f\x05”