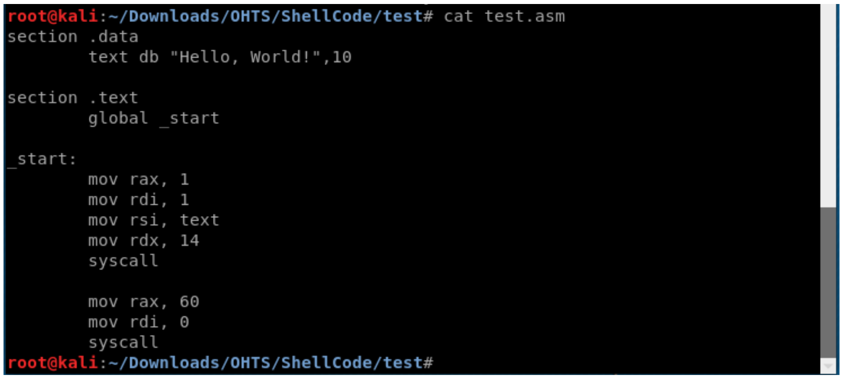
Shell Code

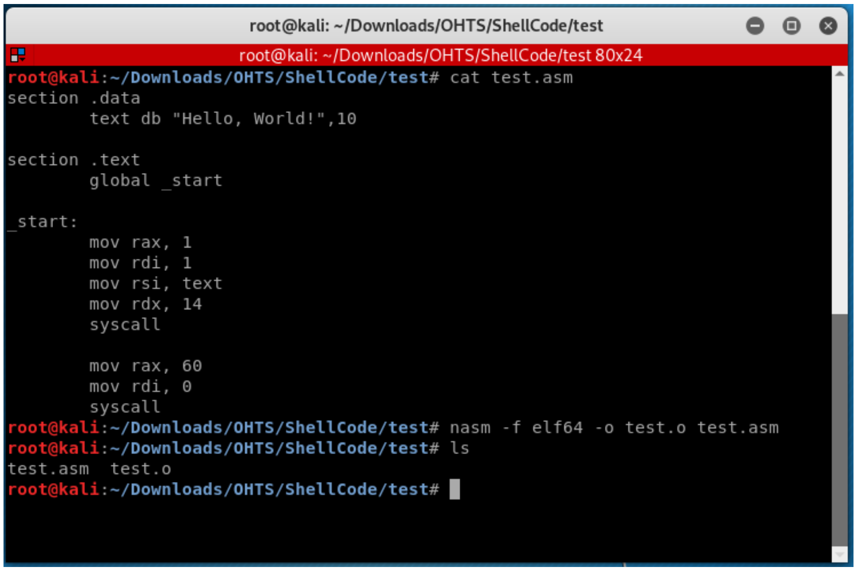
First, we need to create test.asm file by entering the assembly code.



```
root@kali:~/Downloads/OHTS/ShellCode/test# cat test.asm
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
root@kali:~/Downloads/OHTS/ShellCode/test#
```

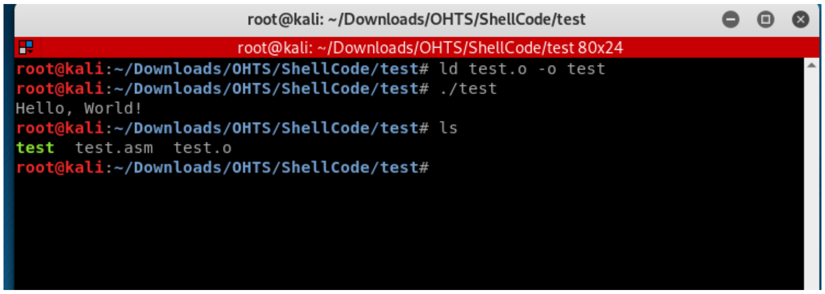
Then we need to create the object file using nasm

Code : nasm -f elf64 -o test.o test.asm


root@kali: ~/Downloads/OHTS/ShellCode/test
root@kali: ~/Downloads/OHTS/ShellCode/test 80x24

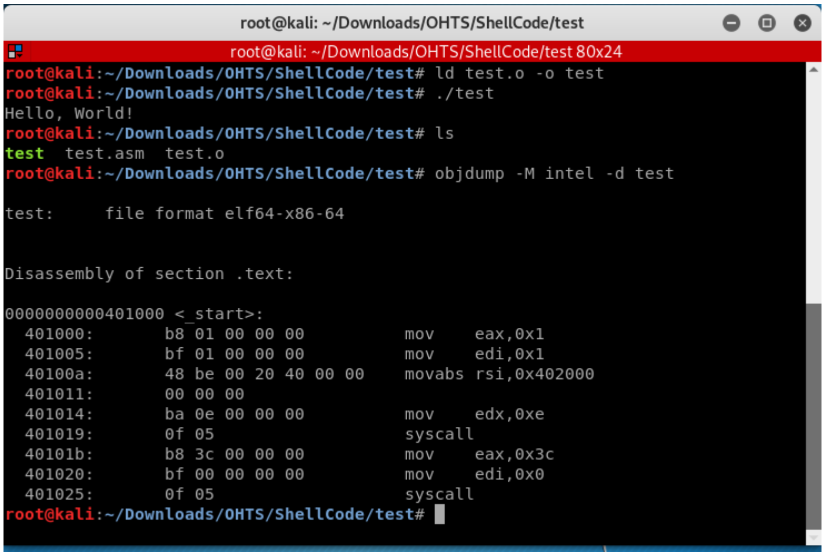
```
root@kali:~/Downloads/OHTS/ShellCode/test# cat test.asm
section .data
        text db "Hello, World!",10

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
root@kali:~/Downloads/OHTS/ShellCode/test# nasm -f elf64 -o test.o test.asm
root@kali:~/Downloads/OHTS/ShellCode/test# ls
test.asm  test.o
root@kali:~/Downloads/OHTS/ShellCode/test# 
```

Then we have to create the executable


root@kali: ~/Downloads/OHTS/ShellCode/test
root@kali: ~/Downloads/OHTS/ShellCode/test 80x24

```
root@kali:~/Downloads/OHTS/ShellCode/test# ld test.o -o test
root@kali:~/Downloads/OHTS/ShellCode/test# ./test
Hello, World!
root@kali:~/Downloads/OHTS/ShellCode/test# ls
test  test.asm  test.o
root@kali:~/Downloads/OHTS/ShellCode/test#
```

Now we can get the Hex dump


root@kali: ~/Downloads/OHTS/ShellCode/test
root@kali: ~/Downloads/OHTS/ShellCode/test 80x24

```
root@kali:~/Downloads/OHTS/ShellCode/test# ld test.o -o test
root@kali:~/Downloads/OHTS/ShellCode/test# ./test
Hello, World!
root@kali:~/Downloads/OHTS/ShellCode/test# ls
test  test.asm  test.o
root@kali:~/Downloads/OHTS/ShellCode/test# objdump -M intel -d test

test:     file format elf64-x86-64


Disassembly of section .text:

0000000000401000 <_start>:
  401000:       b8 01 00 00 00          mov    eax,0x1
  401005:       bf 01 00 00 00          mov    edi,0x1
  40100a:       48 be 00 20 40 00 00    movabs rsi,0x402000
  401011:       00 00 00 
  401014:       ba 0e 00 00 00          mov    edx,0xe
  401019:       0f 05                   syscall 
  40101b:       b8 3c 00 00 00          mov    eax,0x3c
  401020:       bf 00 00 00 00          mov    edi,0x0
  401025:       0f 05                   syscall 
root@kali:~/Downloads/OHTS/ShellCode/test# 
```

“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 ” is the hex dump of the hello world programme