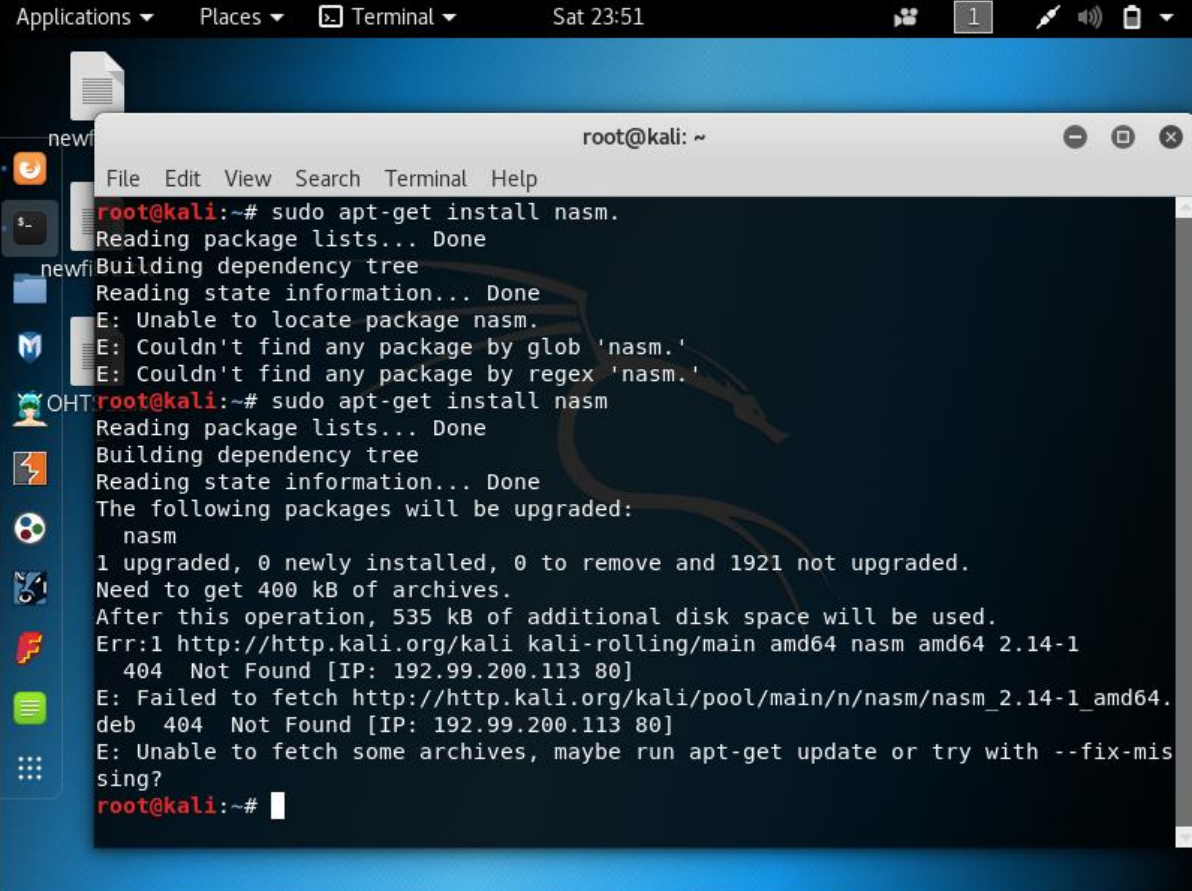


OHTS Lab 2 – Linux Shell Coding

To write the shell codes, knowledge of Assembly and C is needed. Also need to know how the stack works.

Next I google the website called as <https://0x00sec.org/t/linux-shellcoding-part-1-0/289> , in order to go to that website in order to get the shell code.

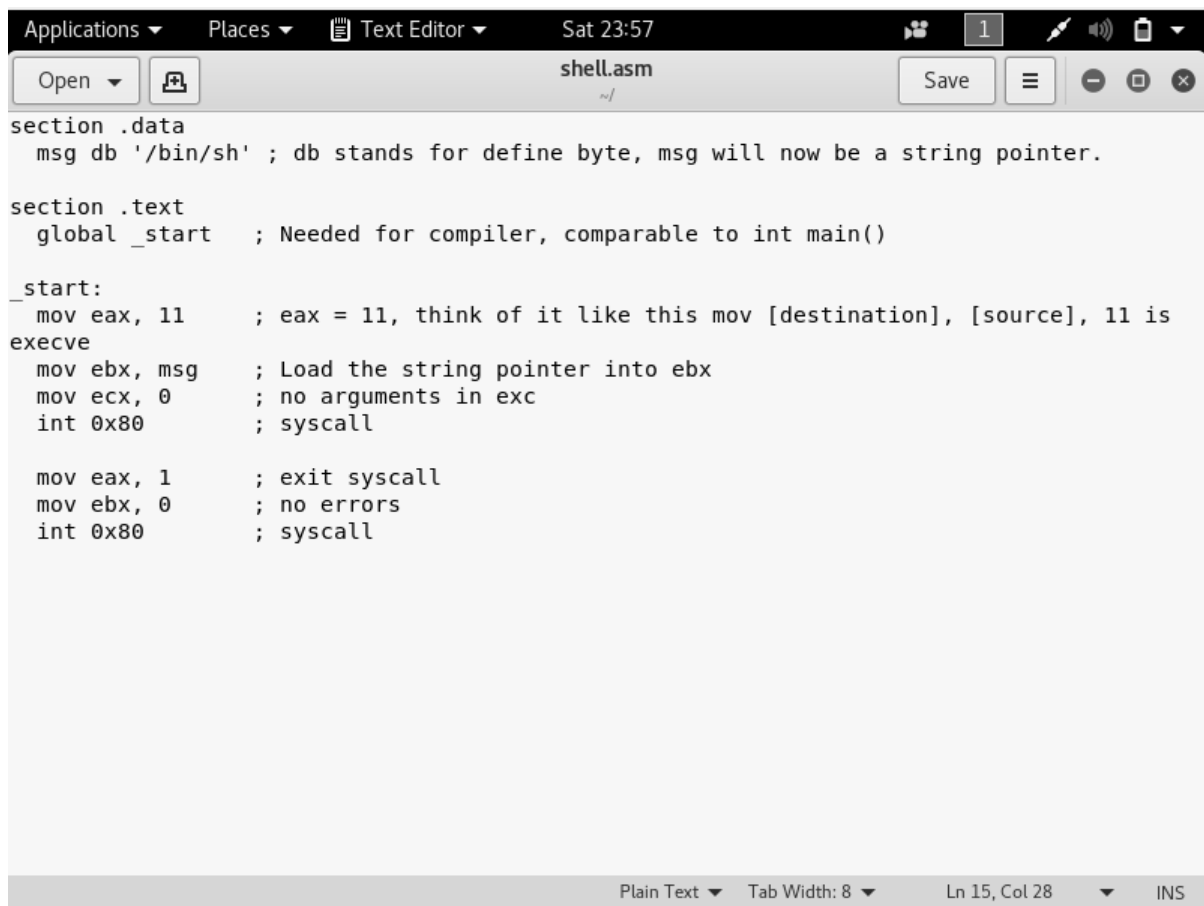
Then, I started the Kali Linux in the Virtual Box, and typed as follows, which is shown in the screen shot (Figure 1) below.



```
Applications ▾ Places ▾ Terminal ▾ Sat 23:51
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo apt-get install nasm.
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package nasm.
E: Couldn't find any package by glob 'nasm.'
E: Couldn't find any package by regex 'nasm.'
root@kali:~# sudo apt-get install nasm
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  nasm
1 upgraded, 0 newly installed, 0 to remove and 1921 not upgraded.
Need to get 400 kB of archives.
After this operation, 535 kB of additional disk space will be used.
Err:1 http://http.kali.org/kali kali-rolling/main amd64 nasm amd64 2.14-1
404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/n/nasm/nasm_2.14-1_amd64.
deb 404 Not Found [IP: 192.99.200.113 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-mis-
sing?
root@kali:~#
```

Figure 1: Install nasm

Then, I copy paste the assembly program in the text editor and save it as shell.asm. This is shown in (Figure 2).



```
Applications ▾ Places ▾ Text Editor ▾ Sat 23:57 1 [Icons]
Open ▾ [Icon] shell.asm Save [Menu] [Zoom In] [Zoom Out] [Close]

section .data
    msg db '/bin/sh' ; db stands for define byte, msg will now be a string pointer.

section .text
    global _start ; Needed for compiler, comparable to int main()

_start:
    mov eax, 11 ; eax = 11, think of it like this mov [destination], [source], 11 is
execve
    mov ebx, msg ; Load the string pointer into ebx
    mov ecx, 0 ; no arguments in exc
    int 0x80 ; syscall

    mov eax, 1 ; exit syscall
    mov ebx, 0 ; no errors
    int 0x80 ; syscall

Plain Text ▾ Tab Width: 8 ▾ Ln 15, Col 28 ▾ INS
```

Figure 2: Save it as shell.asm

Next, to compile this, I typed the following commands. But, it showed me error. So, next I went to Stack overflow to correct the error. Then, I typed as shown in the screen shot (Figure 3).

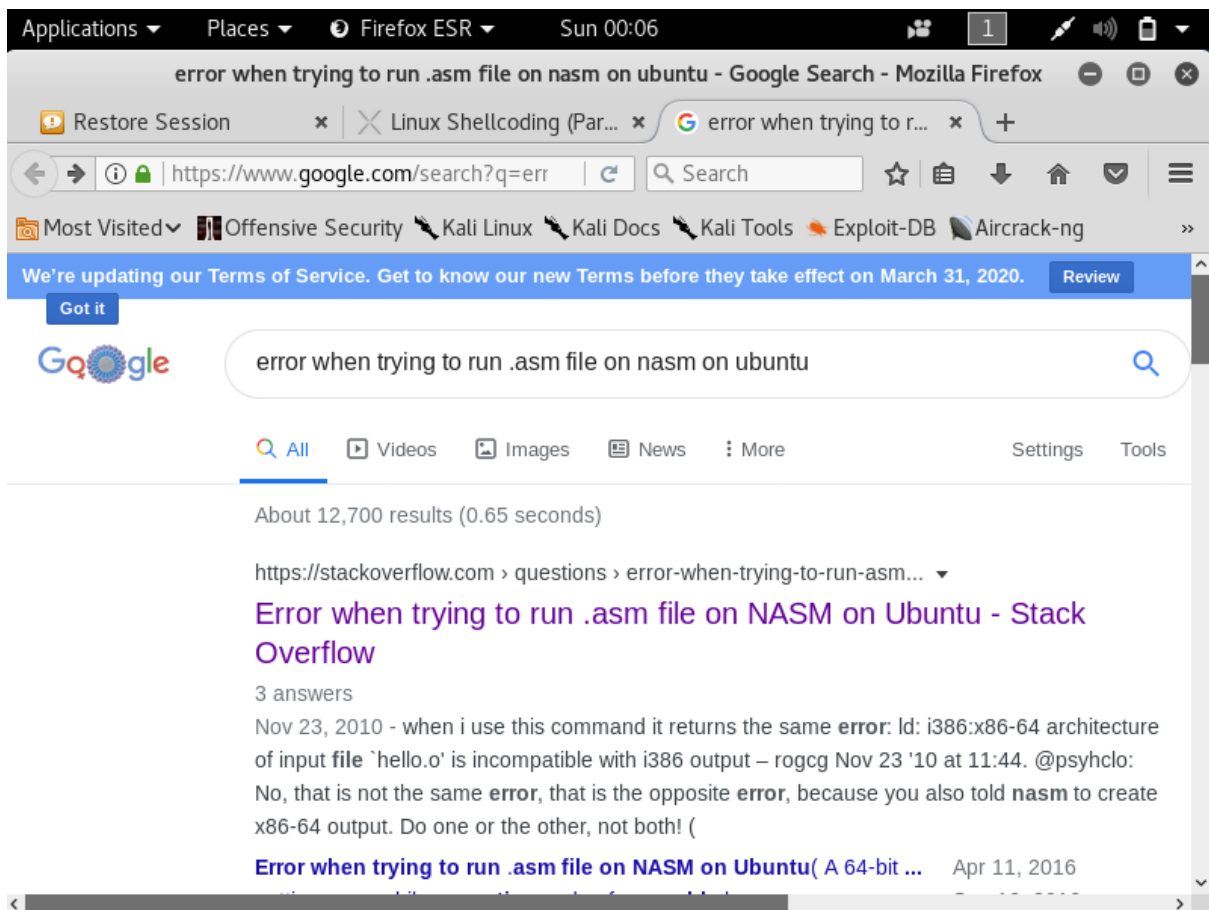
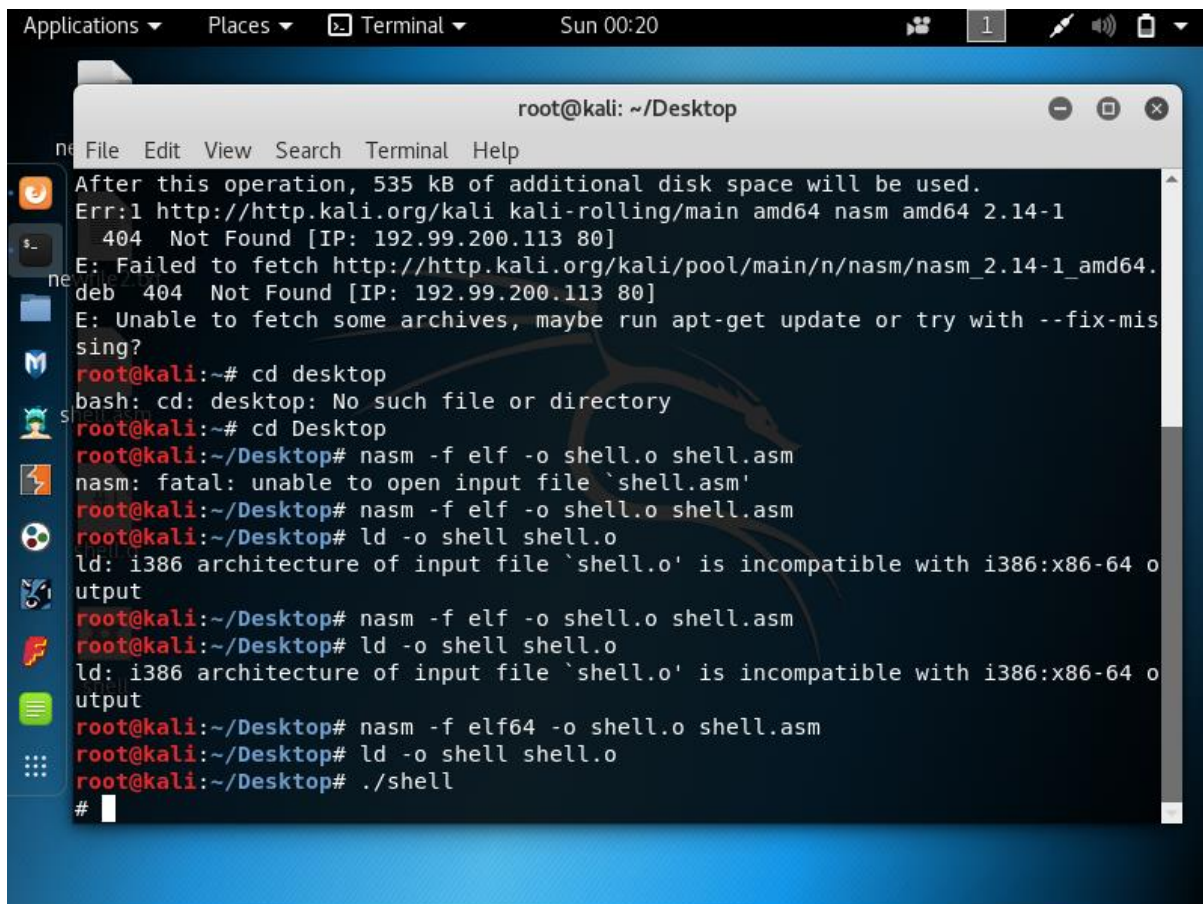


Figure 3: Searching for the error to resolve

Then, as shown in (Figure 4) I typed in the terminal.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
After this operation, 535 kB of additional disk space will be used.
Err:1 http://http.kali.org/kali kali-rolling/main amd64 nasm amd64 2.14-1
404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/n/nasm/nasm_2.14-1_amd64.
deb 404 Not Found [IP: 192.99.200.113 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-mis-
sing?
root@kali:~# cd desktop
bash: cd: desktop: No such file or directory
root@kali:~# cd Desktop
root@kali:~/Desktop# nasm -f elf -o shell.o shell.asm
nasm: fatal: unable to open input file `shell.asm'
root@kali:~/Desktop# nasm -f elf -o shell.o shell.asm
root@kali:~/Desktop# ld -o shell shell.o
ld: i386 architecture of input file `shell.o' is incompatible with i386:x86-64 o
utput
root@kali:~/Desktop# nasm -f elf -o shell.o shell.asm
root@kali:~/Desktop# ld -o shell shell.o
ld: i386 architecture of input file `shell.o' is incompatible with i386:x86-64 o
utput
root@kali:~/Desktop# nasm -f elf64 -o shell.o shell.asm
root@kali:~/Desktop# ld -o shell shell.o
root@kali:~/Desktop# ./shell
#
```

Figure 4: Typed in the terminal

Next, the command which is in the given website <https://0x00sec.org/t/linux-shellcoding-part-1-0/289> gave me error, I changed the “Hello World” command as shown below (Figure 6).

Then, I typed as “linuxcommand.org/lc3_wss0010.php” in the google. And get the command in order to write the first script. This website is shown in (Figure 5).

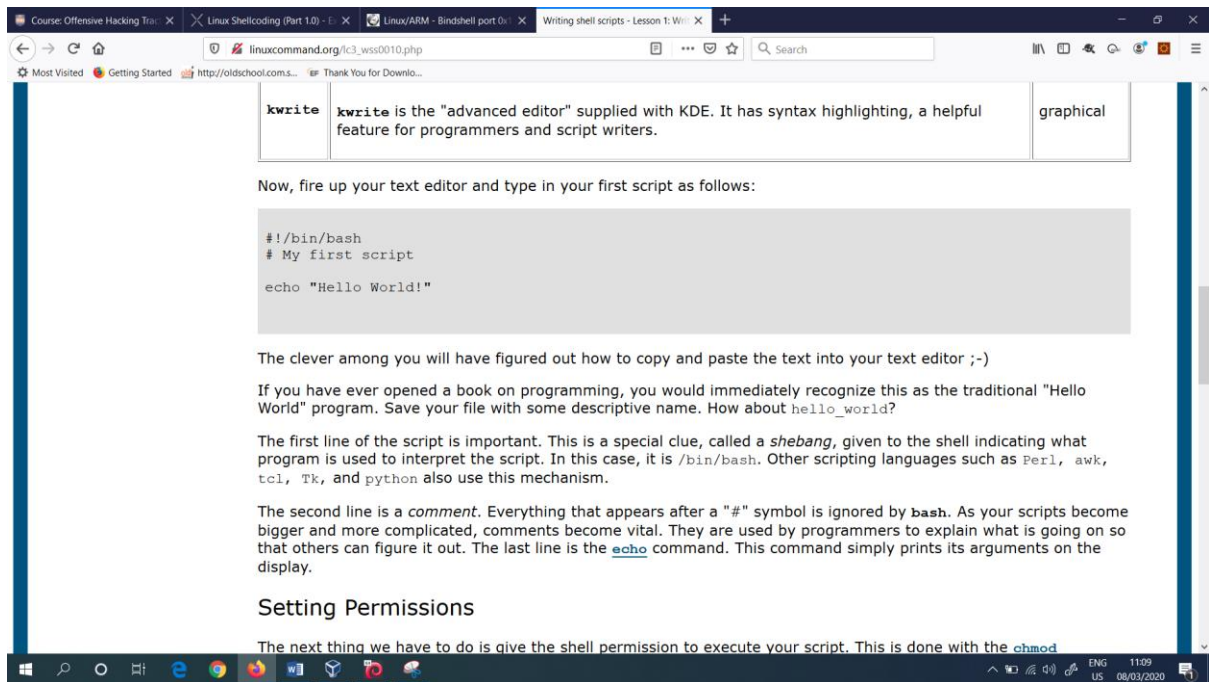


Figure 5: Get the first script

Next, typed the above shown command in the Kali Linux terminal in order to verify whether the same shell code is derived or not (Figure 6).

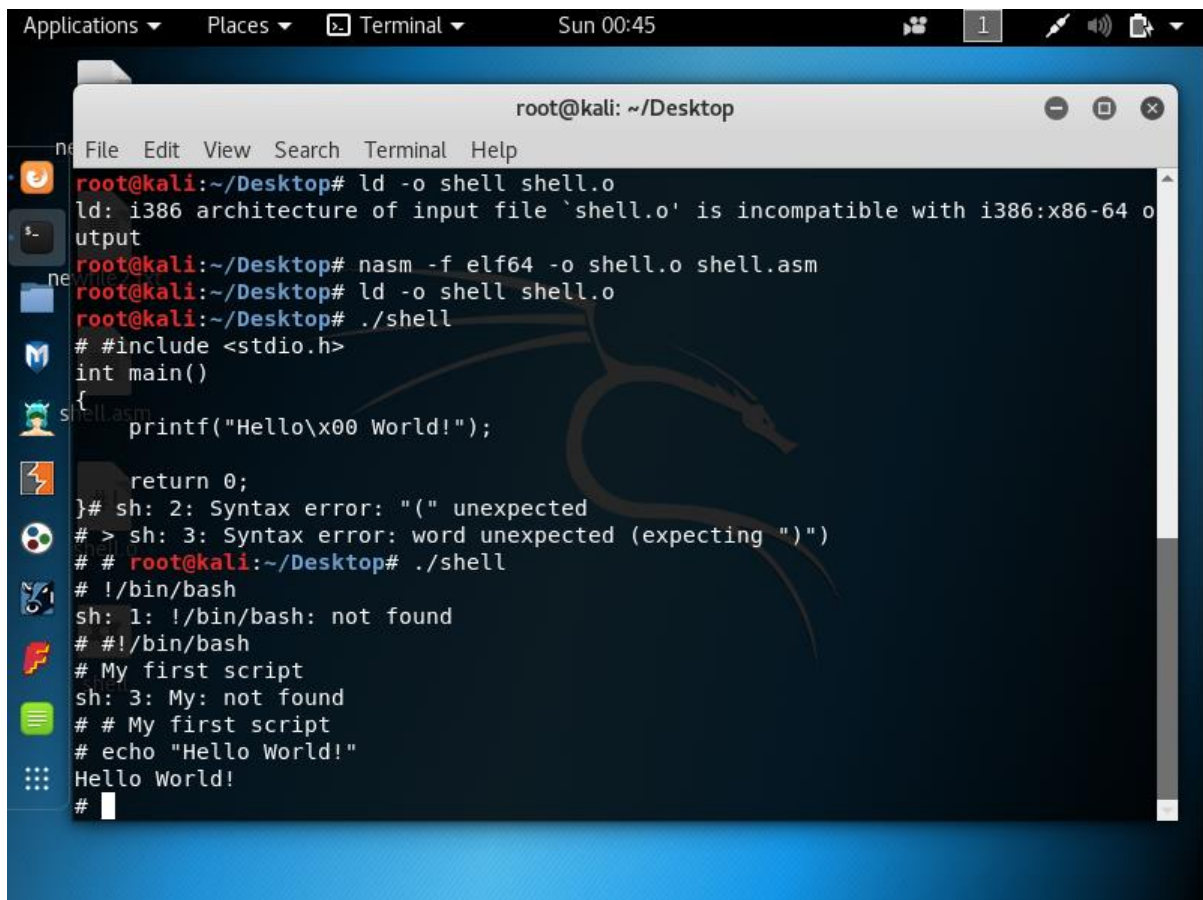
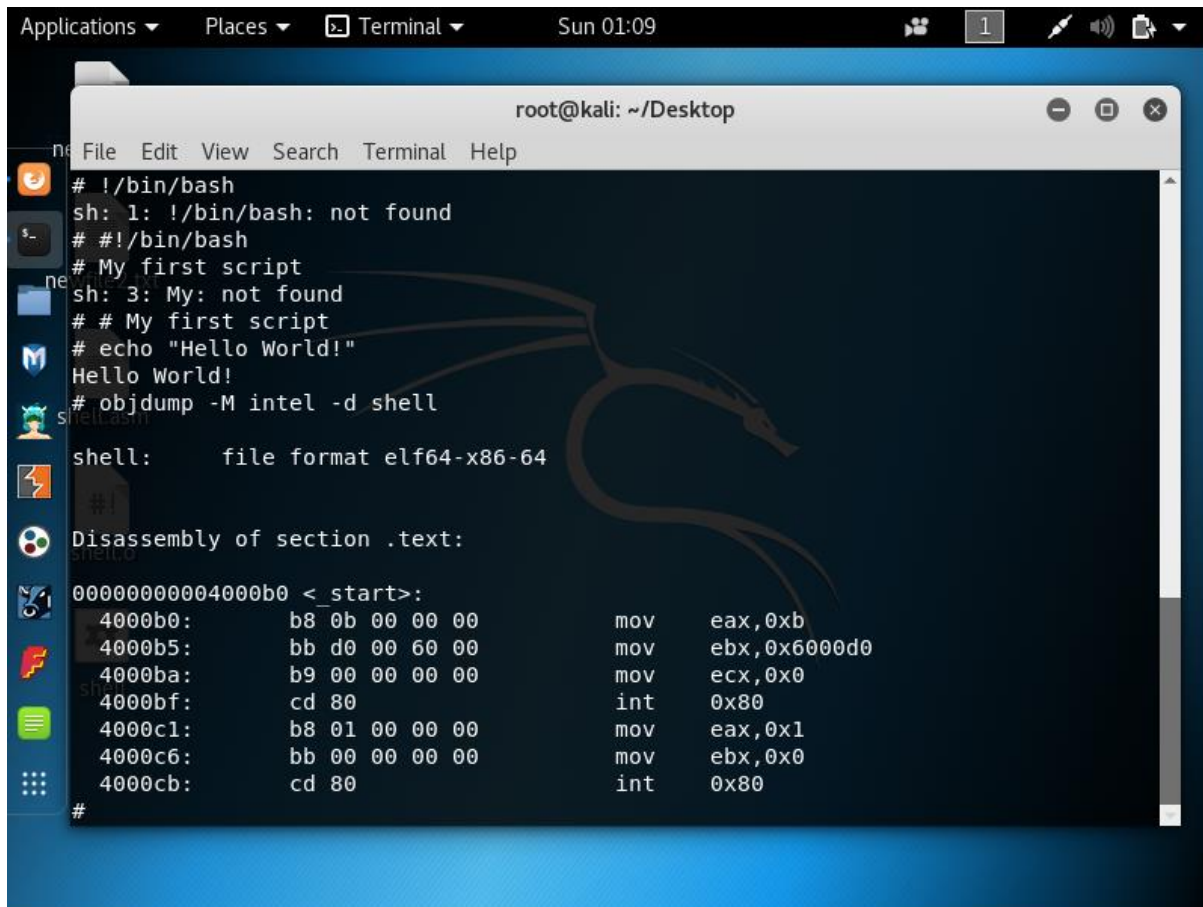


Figure 6: Typed the above command in Kali Linux terminal

Then I typed the command `objdump -M intel -d shell`. Next, it shows me the script code for the file which I saved earlier. The following (Figure 7) shows the following.



```
Applications ▾ Places ▾ Terminal ▾ Sun 01:09
root@kali: ~/Desktop
# ./bin/bash
sh: 1: ./bin/bash: not found
# #./bin/bash
# My first script
sh: 3: My: not found
# # My first script
# echo "Hello World!"
Hello World!
# objdump -M intel -d shell
shell:      file format elf64-x86-64

Disassembly of section .text:
00000000004000b0 <_start>:
4000b0:      b8 0b 00 00 00      mov     eax,0xb
4000b5:      bb d0 00 60 00      mov     ebx,0x6000d0
4000ba:      b9 00 00 00 00      mov     ecx,0x0
4000bf:      cd 80              int     0x80
4000c1:      b8 01 00 00 00      mov     eax,0x1
4000c6:      bb 00 00 00 00      mov     ebx,0x0
4000cb:      cd 80              int     0x80
#
```

Figure 7: Got the shell code

This shell code which I got was as same which is in the <https://0x00sec.org/t/linux-shellcoding-part-1-0/289> website.

So, finally I reverse engineered and I got the same code.