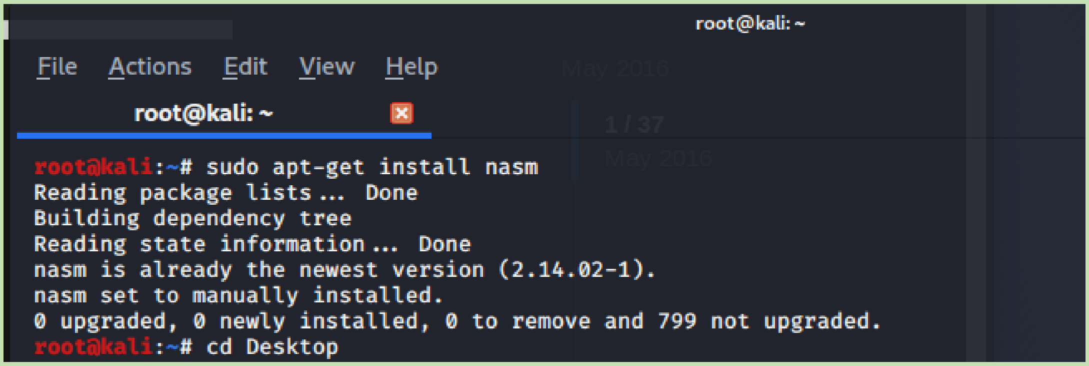
Write a Simple Shellcode

A simple shellcode that spawns a shell

First though, I will write a normal assembly program. I will need nasm installed on my machine to compile it.

Step 1

sudo apt-get install nasm.



```
root@kali:~# sudo apt-get install nasm
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
nasm is already the newest version (2.14.02-1).
nasm set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 799 not upgraded.
root@kali:~# cd Desktop
```

Step 2

Get a sample assembly program

Create a shell.asm file

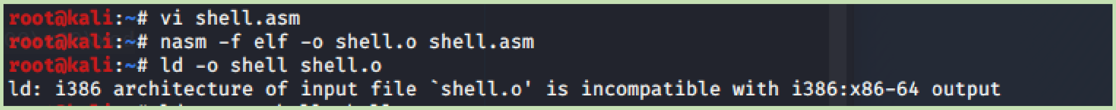
Save that sample assembly program into that shell.asm file

Step 3

To compile it use the following commands:

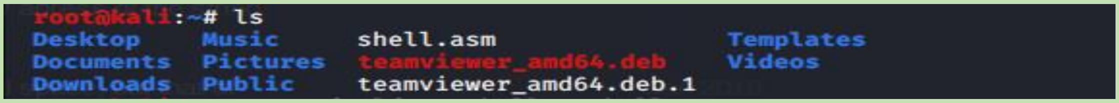
nasm -f elf -o shell.o shell.asm

ld -o shell shell.o

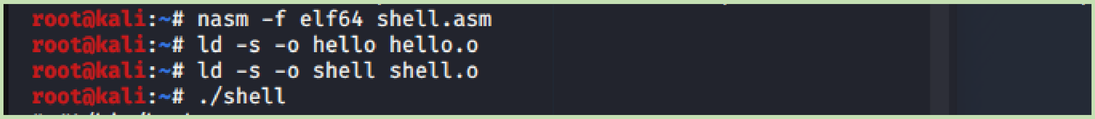


```
root@kali:~# vi shell.asm
root@kali:~# nasm -f elf -o shell.o shell.asm
root@kali:~# ld -o shell shell.o
ld: i386 architecture of input file `shell.o' is incompatible with i386:x86-64 output
```

Check the assembly file is available in root directory using ls command



```
root@kali:~# ls
Desktop    Music     shell.asm                Templates
Documents  Pictures  teamviewer_amd64.deb     Videos
Downloads  Public    teamviewer_amd64.deb.1
```



```
root@kali:~# nasm -f elf64 shell.asm
root@kali:~# ld -s -o hello hello.o
root@kali:~# ld -s -o shell shell.o
root@kali:~# ./shell
```

Step 4

Now run it with:

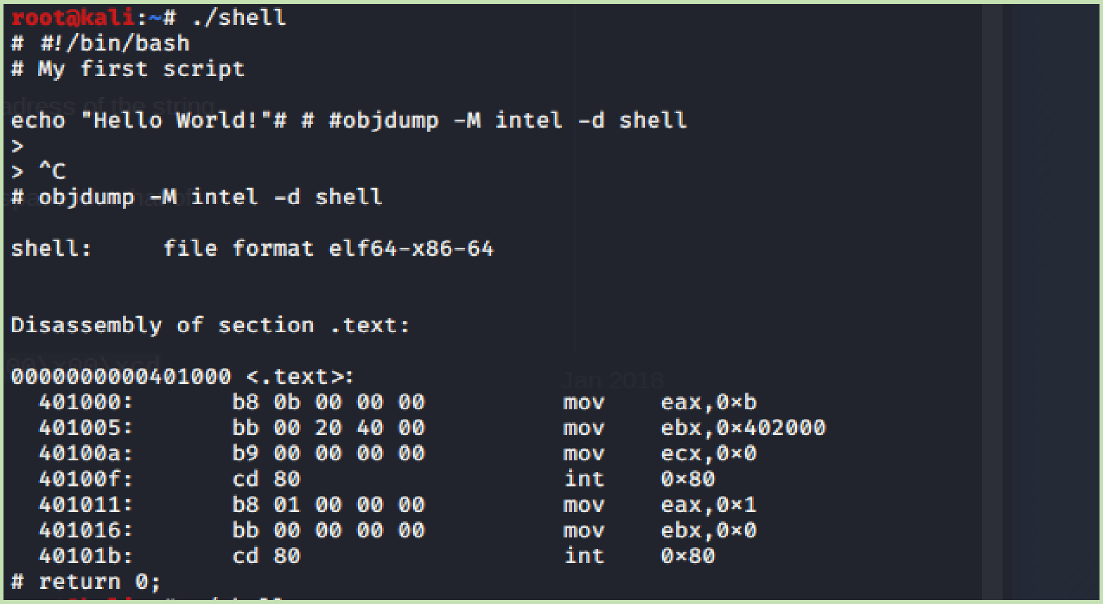
. /shell

Now I can get a shell

Step 5

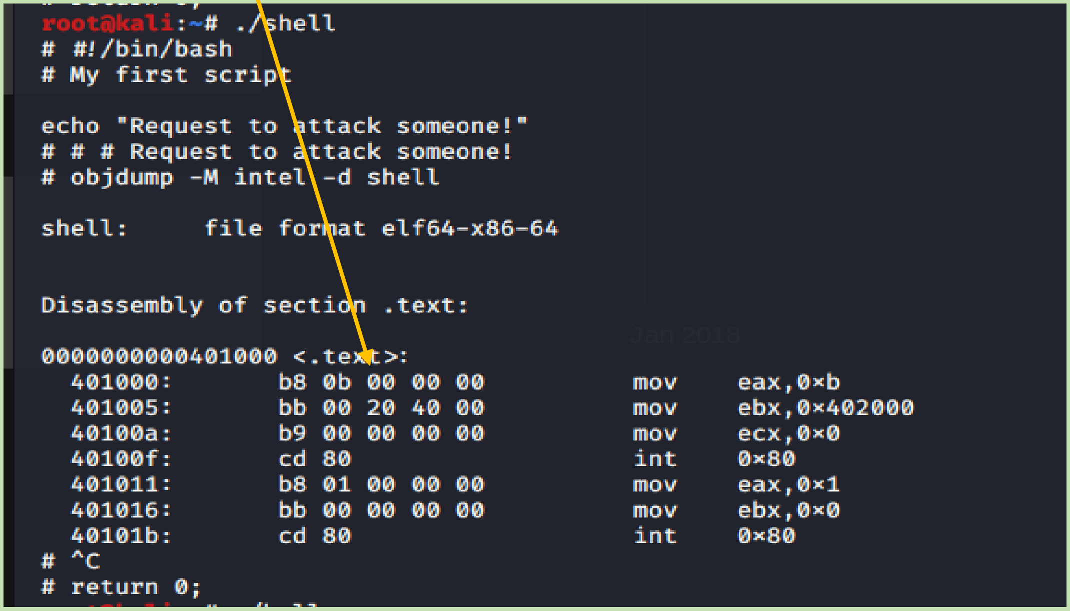
Using the below command to extract the shellcode

objdump -M intel -d shell



```
root@kali:~# ./shell
# #!/bin/bash
# My first script

echo "Hello World!"# # #objdump -M intel -d shell
>
> ^C
# objdump -M intel -d shell

shell:     file format elf64-x86-64


Disassembly of section .text:

0000000000401000 <.text>:
  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
# return 0;
```

Here I got the shell code



```
root@kali:~# ./shell
# #!/bin/bash
# My first script

echo "Request to attack someone!"
# # # Request to attack someone!
# objdump -M intel -d shell

shell:     file format elf64-x86-64


Disassembly of section .text:

0000000000401000 <.text>:
  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
# ^C
# return 0;
```

THANK YOU