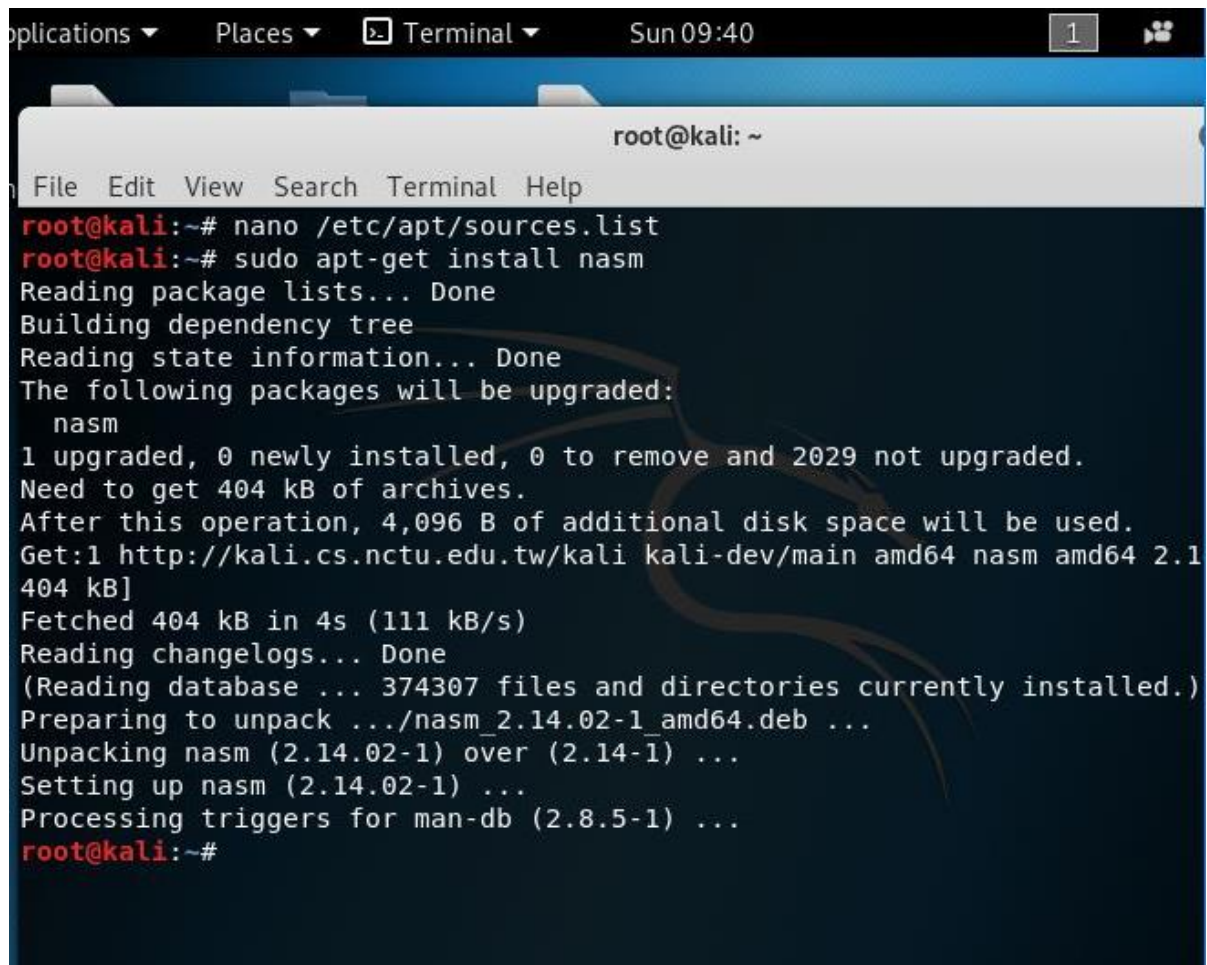


ShellCode

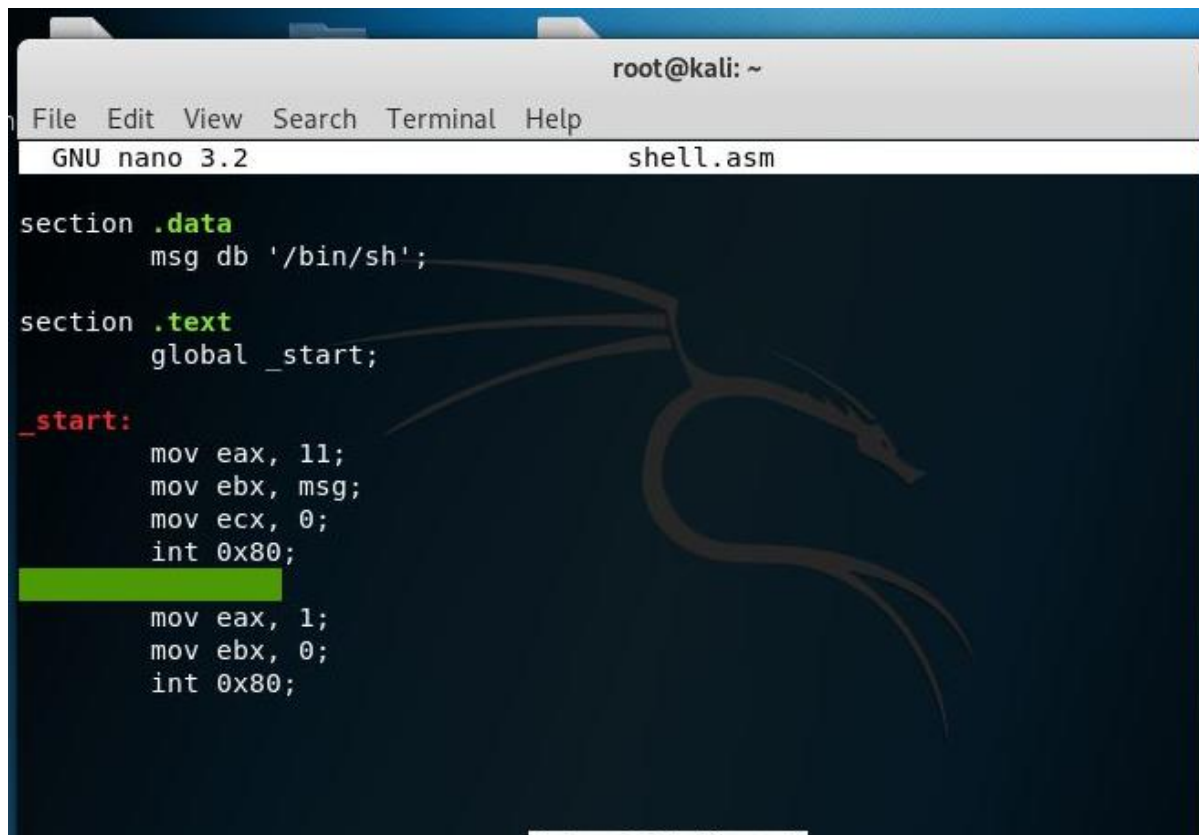
Part 1

First, nasm needs to be installed.



```
Applications ▾ Places ▾ Terminal ▾ Sun 09:40 1
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nano /etc/apt/sources.list
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 2029 not upgraded.
Need to get 404 kB of archives.
After this operation, 4,096 B of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-dev/main amd64 nasm amd64 2.14.02-1 [404 kB]
Fetched 404 kB in 4s (111 kB/s)
Reading changelogs... Done
(Reading database ... 374307 files and directories currently installed.)
Preparing to unpack .../nasm_2.14.02-1_amd64.deb ...
Unpacking nasm (2.14.02-1) over (2.14-1) ...
Setting up nasm (2.14.02-1) ...
Processing triggers for man-db (2.8.5-1) ...
root@kali:~#
```

The shell.asm Assembly program:

A screenshot of a terminal window on a Kali Linux system. The window title is 'root@kali: ~'. The terminal shows the GNU nano 3.2 editor editing a file named 'shell.asm'. The code in the file is as follows:

```
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;
```

The code defines a data section with a message string, a text section with a global start label, and the start routine which uses the syscalls 11 (write) and 1 (exit) to execute a shell. A faint dragon logo is visible in the background of the terminal window.

Compiling and running the shell:

```
root@kali: ~  
h File Edit View Search Terminal Help  
ld: i386 architecture of input file `shell.o' is incompatible with i386:  
output  
root@kali:~# ld -o shell shell.o -m elf_i386  
root@kali:~# ./shell  
#  
#  
# ^Z^C  
#  
# ^A^C  
#  
root@kali:~# nano shell.asm  
root@kali:~# nasm -f elf -o shell.o shell.asm  
root@kali:~# ld -o shell shell.o -m elf_i386  
root@kali:~# ./shell  
# hello  
sh: 1: hello: not found  
# 1  
sh: 2: 1: not found  
# 0  
sh: 3: 0: not found  
# ls  
Desktop      Downloads  Pictures  Templates  ca  shell      shell.o  
Documents    Music      Public    Videos     cb  shell.asm  
#
```

Extracting the shellcode:

```
root@kali: ~  
File Edit View Search Terminal Help  
sh: 2: 1: not found  
# 0  
sh: 3: 0: not found  
# ls  
Desktop    Downloads  Pictures  Templates  ca  shell    shell.o  
Documents  Music      Public    Videos    cb  shell.asm  
#  
root@kali:~# nano shell.asm  
root@kali:~# objdump -M intel -d shell  
  
shell:      file format elf32-i386  
  
Disassembly of section .text:  
  
08049000 <_start>:  
  8049000:    b8 0b 00 00 00      mov     eax,0xb  
  8049005:    bb 00 a0 04 08      mov     ebx,0x804a000  
  804900a:    b9 00 00 00 00      mov     ecx,0x0  
  804900f:    cd 80              int     0x80  
  8049011:    b8 01 00 00 00      mov     eax,0x1  
  8049016:    bb 00 00 00 00      mov     ebx,0x0  
  804901b:    cd 80              int     0x80  
root@kali:~#
```