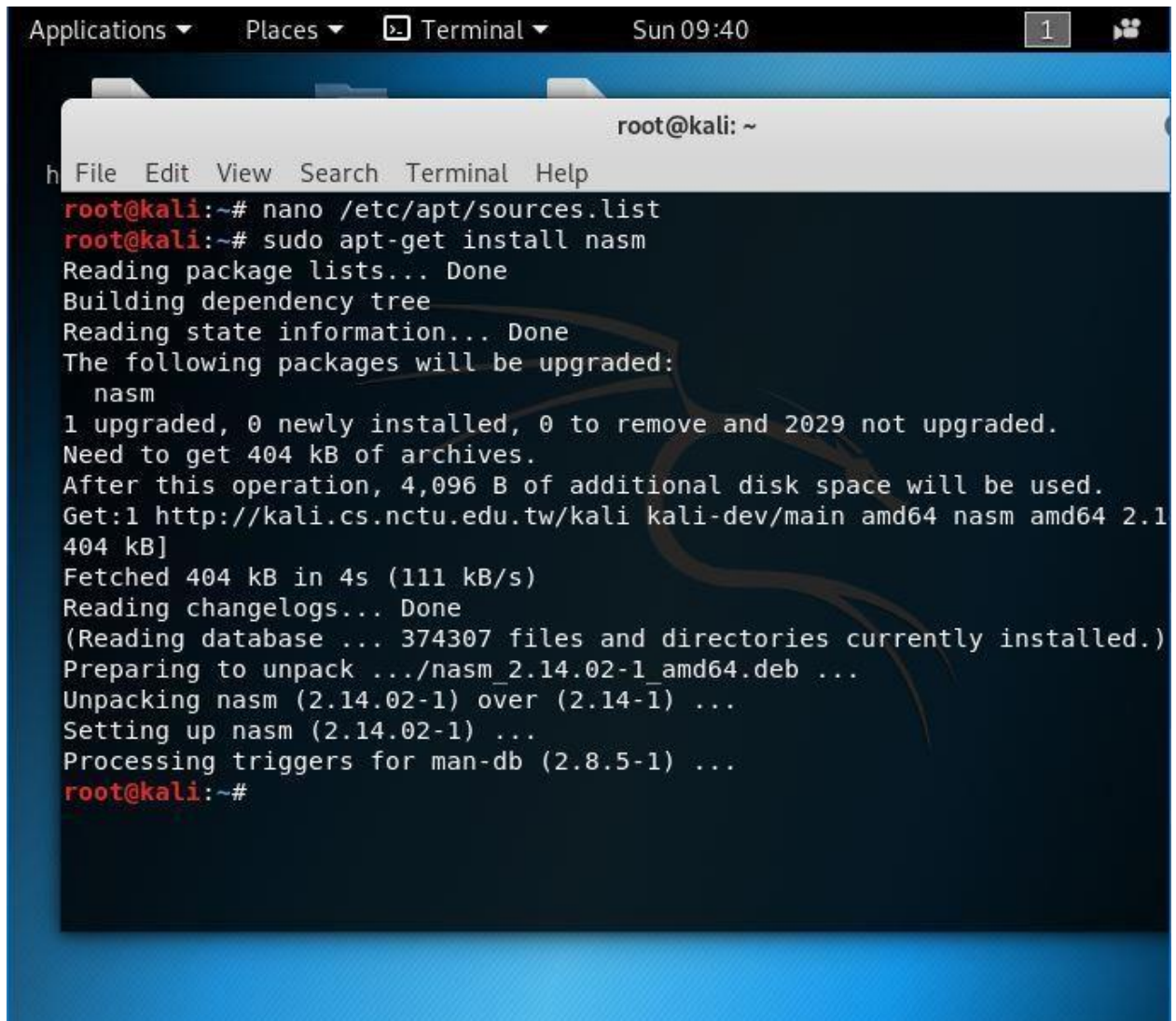


# ShellCode

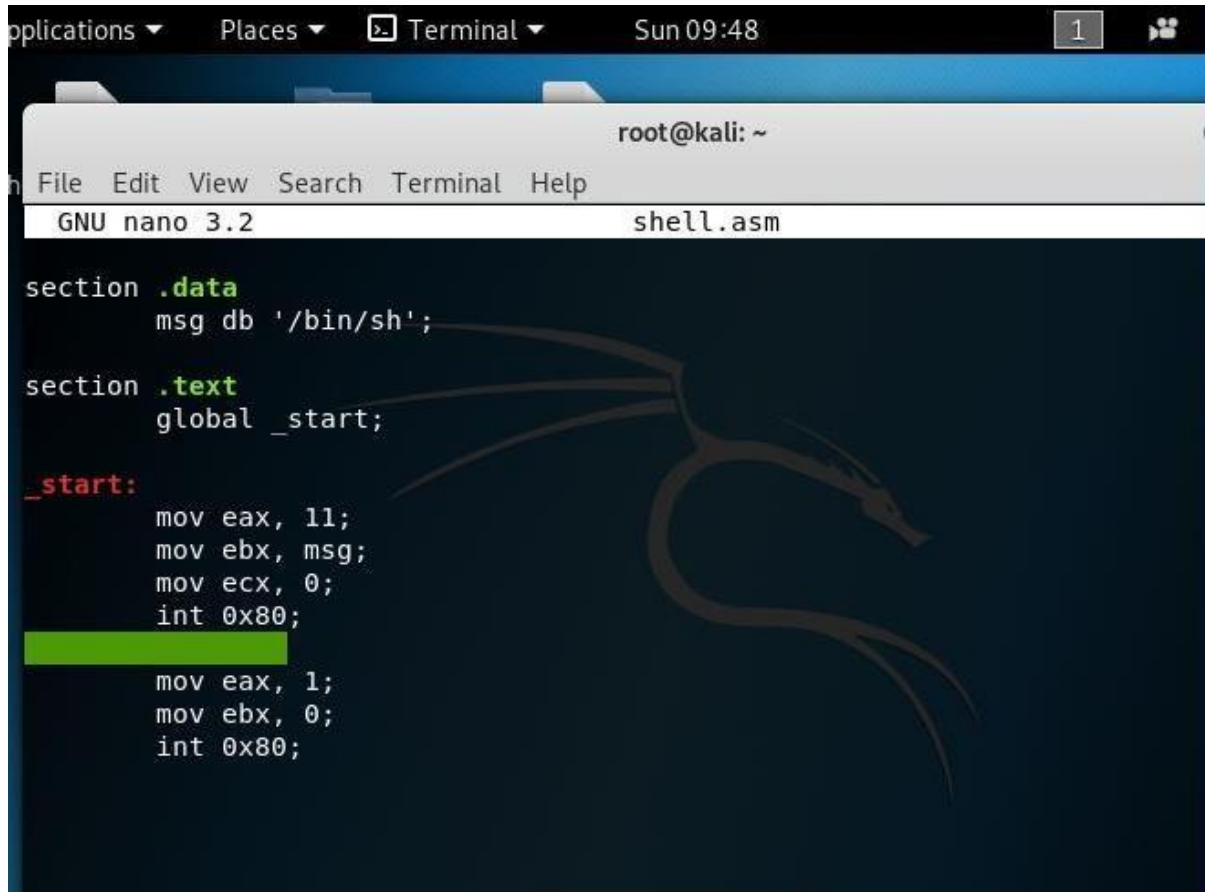
## Part 1

Installing nasm:

A terminal window titled 'root@kali: ~' is shown within a desktop environment. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows the user running 'nano /etc/apt/sources.list' and 'sudo apt-get install nasm'. The system then displays the package lists, builds the dependency tree, and shows that nasm will be upgraded. It indicates that 404 kB of archives are needed and that 4,096 B of additional disk space will be used. The source is listed as 'http://kali.cs.nctu.edu.tw/kali kali-dev/main amd64 nasm amd64 2.14.02-1'. The package is fetched, changelogs are read, and the database is updated. Finally, nasm (2.14.02-1) is unpacked and set up, and triggers for man-db (2.8.5-1) are processed.

```
Applications ▾ Places ▾ Terminal ▾ Sun 09:40 1
root@kali: ~
h 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:~#
```

This is the assembly program: shell.asm

A screenshot of a terminal window on a Kali Linux system. The terminal title bar shows 'Sun 09:48' and a tab labeled '1'. The window content shows the nano text editor editing a file named 'shell.asm'. The editor's status bar at the top indicates 'GNU nano 3.2' and the current file 'shell.asm'. The assembly code is as follows:

```
section .data
    msg db '/bin/sh';

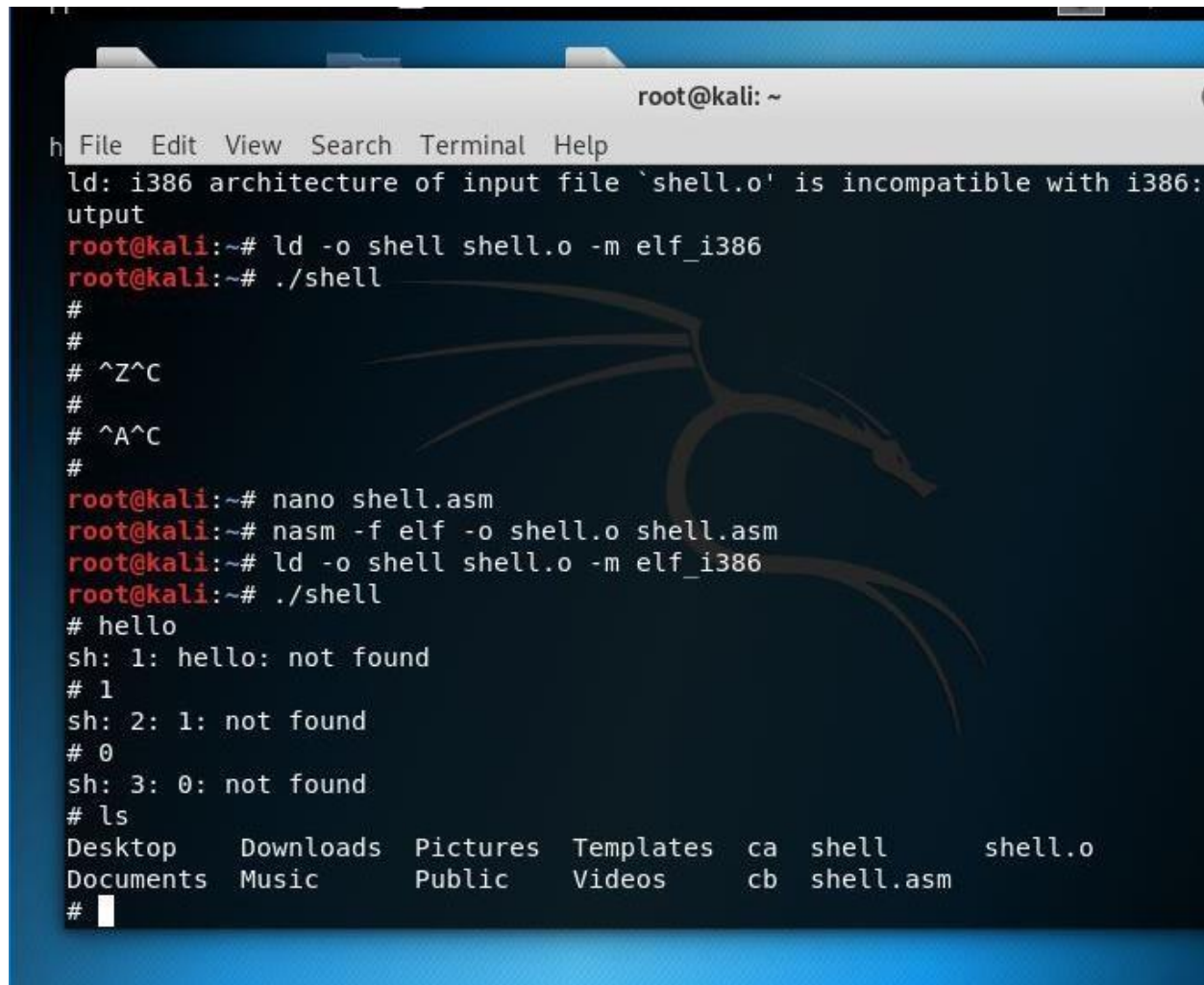
section .text
    global _start;

_start:
    mov eax, 11;
    mov ebx, msg;
    mov ecx, 0;
    int 0x80;

    mov eax, 1;
    mov ebx, 0;
    int 0x80;
```

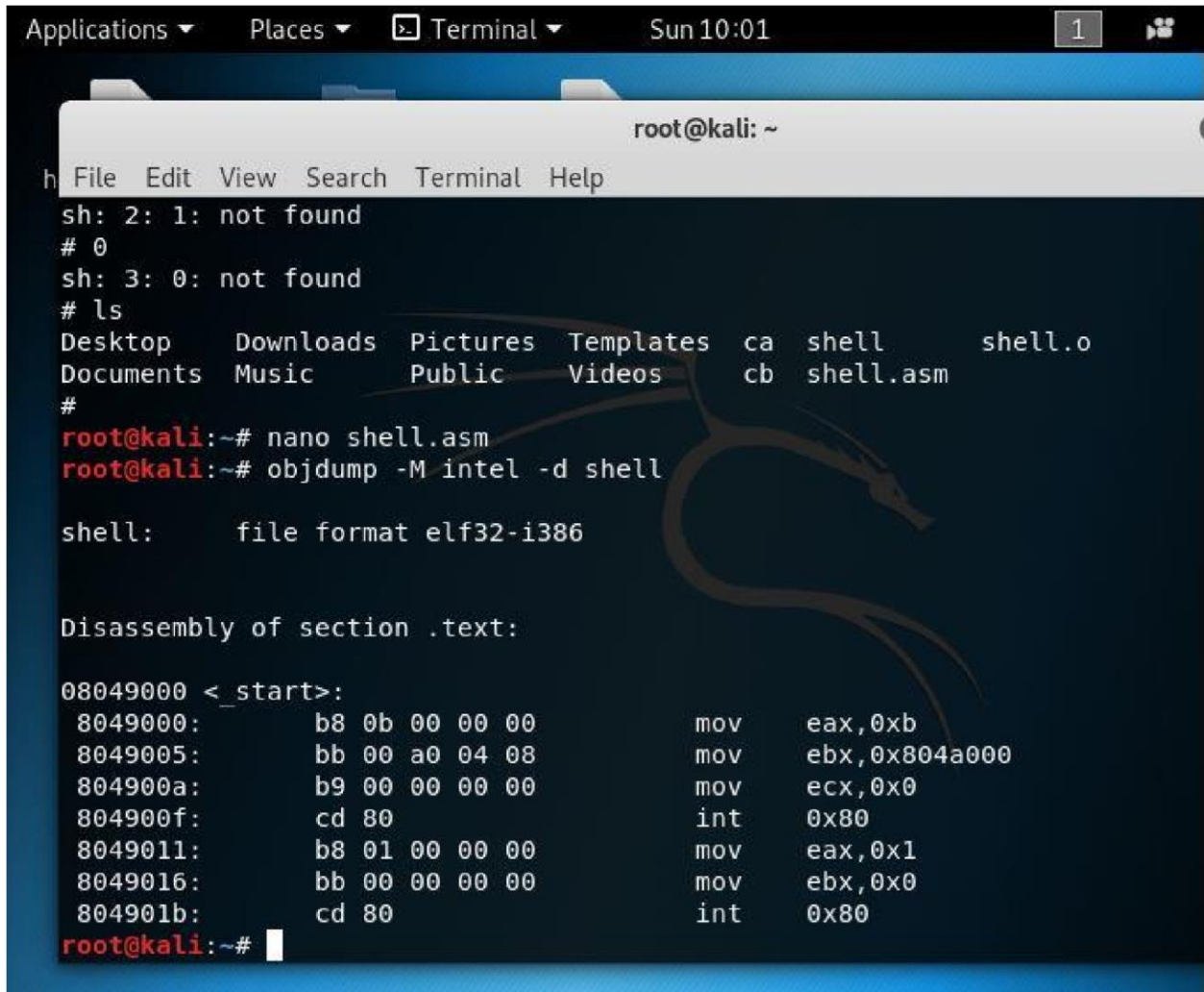
The code defines a data section with a message string, a text section with a global start symbol, and the start routine which uses the int 0x80 instruction to execute a system call. The first call uses eax=11 and ebx=msg, while the second call uses eax=1 and ebx=0. A faint dragon logo is visible in the background of the terminal window.

Compiling and running the shell:

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the compilation of a custom shell. It starts with an error: 'ld: i386 architecture of input file `shell.o' is incompatible with i386: output'. The user then runs 'ld -o shell shell.o -m elf\_i386' and './shell'. The shell prompts with '#'. The user enters '^Z^C' and '^A^C'. Then, the user runs 'nano shell.asm', 'nasm -f elf -o shell.o shell.asm', and 'ld -o shell shell.o -m elf\_i386'. The shell is run again with './shell'. It prompts with '# hello', then 'sh: 1: hello: not found'. The user enters '1', and it prompts 'sh: 2: 1: not found'. The user enters '0', and it prompts 'sh: 3: 0: not found'. The user enters 'ls', and it shows a directory listing: Desktop, Downloads, Pictures, Templates, ca, shell, shell.o, Documents, Music, Public, Videos, cb, shell.asm. The prompt is '# ' with a cursor.

```
root@kali: ~
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:



The screenshot shows a terminal window on a Kali Linux system. The window title is "root@kali: ~". The terminal output shows the following commands and results:

```
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:~#
```

Shell code:

“\xba\x01\x00\x00\x00\xb9\x00\x20\x40\x00\xbb\x01\x00\x00\x00\xb8\x04\x00\x00\xcd\x80\xb8\x01\x00\x00\x00\xcd\x80”