Cyber Youth Singapore

ezpz

horizontal line

**Creator Name: Kok Rui**

# Setup:

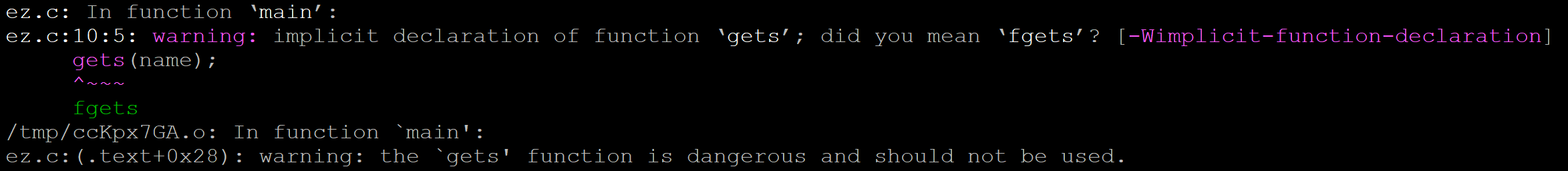
## **Static Files:**

* 1. ez.c (source for participants)
  2. ez (binary for participants)
  3. ezreal (binary @ host)

## **Usage:**

* 1. Host chall: nohup sudo tcpserver -t 50 -RHl0 0.0.0.0 <port> ./ezreal
  2. In CTFd, give participants ez.c and ez

# Description:

* **Description:**
  + Guess the password!
  + Give them the netcat command here thx
* **Hint:**
  + You don’t need (and in fact, can never) guess the password…
  + When I compiled the program, it told me this: 

# Solution

1. Basic bof. 29th char will overwrite “success” - if participants’ level of understanding is just knowing that a buffer overflow is just more characters, then just anyhow whack extra characters, they will get flag