Canary Keeper

Challenge

My friend gave me this executable, but it keeps giving me errors. Can you get the flag?

Solution

We are given a binary which we can take a look at in Ghidra. At first glance it looks like the main function lets the user input a 73 bytes long string using gets, which immediatley made me curios. After reading input from the user, it uses strcmp to check if the variable below the user input on the stack is `canary`. That made me think that we need to overflow the user input field, but make sure I don't modify the stack canary. After that, it uses strcmp again to check if the next varibable is the string `FLAG`.

My first attempt was to use a Python2 payload: `python2 -c 'b"A" * 73 + b"canary" + b"FLAG"'`. Here I filled the 73 bytes buffer and added the string canary and FLAG. However that didn't seem to work. I then remebered strcmp compares until the next null terminator. I didn't rembember how I could add a null byte in my Python2 payload, so switched to using pwntools in Python3. After the canary string I added a p64 with a nullbyte.

An added benefit with using pwntools is that I could automatically send the payload. See solution below.

Flag: bcactf{s1mple_CANaRY_9b36bd9f3fd2f}

Python

We need to specify the session cookie to validate the captcha, else we will recieve "Invalid captcha".

```
from pwn import *

io = remote('challs.bcactf.com', 32101)

payload = b'A' * 73 + b'canary' + p64(0x0) + b'FLAG'

io.sendline(payload)

io.recvuntil(b'Flag: ')

print(io.recvall().decode())
```