**RE lab 08 - Heap Exploitation**

**Lab files and setup**

Download the lab files from [here](https://pwnthybytes.ro/unibuc_re/08-lab-files.zip). The archive password is infected.

* Install pwngdb from [here](https://github.com/scwuaptx/Pwngdb). It is an extra plugin on top of gdb/peda which provides extra commands provided that you install debugging symbols for libc.

**Useful pwngdb commands**

* Tracing malloc/frees

gdb-peda$ tracemalloc on

Breakpoint 1 at 0x7ffff7a782d0: file malloc.c, line 3521.

Breakpoint 2 at 0x7ffff7a76c60: file malloc.c, line 4139.

Breakpoint 3 at 0x7ffff7a79490: file malloc.c, line 4663.

Breakpoint 4 at 0x7ffff7a796e0: file malloc.c, line 4502.

gdb-peda$ c

Continuing.

malloc(0x1000) = 0x4052e0

malloc(0x68) = 0x4062f0

malloc(0x3039) = 0x406360

* Viewing all allocated/freed chunks and their status using only heap data (heuristics, so may fail)

gdb-peda$ parseheap

addr prev size status fd bk

0x405000 0x0 0x250 Used None None

0x405250 0x0 0x80 Used None None

0x4052d0 0x0 0x1010 Used None None

0x4062e0 0x0 0x70 Used None None

0x406350 0x0 0x3050 Used None None

* Viewing freed chunks and their status using linked list data (from libc, very reliable)

gdb-peda$ heapinfo

(0x20) fastbin[0]: 0x0

(0x30) fastbin[1]: 0x0

(0x40) fastbin[2]: 0x0

(0x50) fastbin[3]: 0x0

(0x60) fastbin[4]: 0x0

(0x70) fastbin[5]: 0x0

(0x80) fastbin[6]: 0x0

top: 0x4093a0 (size : 0x1cc60)

last\_remainder: 0x0 (size : 0x0)

unsortbin: 0x0

(0x80) tcache\_entry[6]: 0x405260

**Tasks**

**Task 1**

* Create an automation function for each program function in order to use them programmatically. **(2p)**
* Using the vulnerability and the description in the course, create a Write-What-Where primitive. **(2p)**
* Use one of the proposed exploitation routes for this primitive given in the previous course to spawn a shell. Remote end: 45.76.91.112 10081 **(6p)**

**Task 2**

* Create an automation function for each program function in order to use them programmatically. **(2p)**
* Recover the password from the freed chunk in order to spawn a shell. Remote end: 45.76.91.112 10082 **(4p)**