CS341 Fall 2007 Lab #11

Heap-overflow attacks are not as well known as their stack-overflow counterparts. However, they possess much greater potential of compromising a diverse set of targets in addition to return addresses in the stack. This lab explores the basics of Doug Lea's classical malloc algorithm and an exemplary heap-overflow attack based on it.

Read this: http://www.phrack.org/issues.html?issue=57&id=9#article
After gaining some basic understanding on the subject, read heap_overflow.c along with its corresponding assembly, heap_overflow.asm. You can find both files on the class website. The file, heap_overflow.c, implements the so-called “double free attacks” and launches a shell when the attack succeeds. You are not able to try this program on any CS machines on your own because the newer version libc has stemmed this particular vulnerability, and all CS machines have been upgraded and equipped with the newer libc. Nonetheless, the file output shows what you will see when heap_overflow.c runs on an older machine.

Answer the following questions.

1) *What and where is the target this particular attack tries to overwrite?*

2) *What address does this attack overwrite the target with? And why does this cause the launch of the shell?*

3) *Construct the heap picture* ***before*** *the attack happens (you only need to cover those two chunks malloc'd in the program).*

4) *Construct the heap picture* ***after*** *the attack happens (you only need to cover those two chunks malloc'd in the program).*