Training 2 - Buffer Overflow

Loïc Delestra

For this training we will use an online lab.
http://overthewire.org/wargames is an online lab providing wargames. Narnia is a wargame based on binary exploitation. The game is divided in 10 levels. You start at level 0 with the user narnia0. To lvlup you need to find creditentials to the next level user, in this case le password for user narnia1. The password to access next level is stored into a file `/etc/narnia_pass/narnia<lvl+1>`.

A/ First steps. Feel the memory

Your goal is to read /etc/narnia__pass/narnia1 and get the password for narnia1 user.
You will need to use a buffer overflow on a variable to modify another one value's to `0xdeadbeef` .

1. Open a terminal and access to `narnia.labs.overthewire.org` through ssh with user `narnia0` and password `narnia0`.
2. Go to /narnia/ and open the narnia0.c file.
   What are the variables allocated in the stack ?
3. Execute narnia0 binary. What is the output ?
   Execute narnia0 again with the string 'BBBBBBBBBBBBBBBBBBBBBBBBBBBBB' as input. What is the variable "val" new value ? What is the ASCII code for 'B'.
4. Modify your input string to set the value `0xdeadbeef` in the "var" variable.
5. When "var" is correctly set, you get a shell with narnia1 user rights and you can `cat /etc/narnia_pass/narnia1` to get the password.

B/ Second step.

Use your new creditential to login as narnia1. And you are ready to start the next level with the binary /narnia/narnia1 exploitation. clue: Use shellcode from `http://shell-storm.org/shellcode/`