Quiz 2

Exploit these binaries

Generic Instructions

In this quiz you are given a set of binaries and you are requested to exploit them, using different techniques for each binary.

Setup

You will need to be physically present in the lab class of the course, in your time slot. You are free to use everything (including searching the Internet), but you are not allowed to cooperate. You need to work with the binaries on the Unix lab (at a machine like 103ws1, 103ws2, etc.) and to set up your environment correctly. You will also need BlackBoard to submit your solutions on time. Only solutions submitted through BlackBoard, and on time, will be accepted. Points will be deducted in the case of delayed submissions.

IMPORTANT: Setting up the environment

This part should be tested before the quiz. **Questions about this part will not be answered during the quiz.**

For running and experimenting with the binaries you need to set up your environment accordingly. The easiest way to do this, is to use the following scripts. For gdb, add the following lines in your `$HOME/.gdbinit`:

```
unset environment
set env TEMP=1000
set exec-wrapper setarch i686 -R -3
```

If you now want to run any binary without gdb, the following script can be useful:

```
#! /bin/sh
env -i TEMP=1000 setarch i686 -R -3 $@
```

Assuming your script is called `run.sh` and it is executable, then invoking a binary can be done in the following fashion:

```
$ ./run.sh ./bin.0 input
```

Do not try to run the binaries differently; you will most likely experience crashes and you will not be able to complete the tasks. In order to test the environment there is a binary (not exploitable) that you can use at:

https://srec.cs.ucy.ac.cy/epl326/quiz2/test/bin.0

Getting the binaries

The binaries will be given during the quiz and there will be different for each group. The binaries will be given through a URL. You must be able to download and copy all the four binaries in your home directory in your Unix lab. For testing this, try with the sample binary above.

NOTE: If you download and copy a binary to your home directory, the permissions may change. Make sure your binary is executable (use chmod and +x).

For testing that you can download and execute the test binary, do the following.

Download the binary:

```
$ wget --no-check-certificate https://srec.cs.ucy.ac.cy/epl326/quiz2/test/bin.0
```

Make it executable:

```
$ chmod a+x ./bin.0
```

Run it:

```
$ ./run.sh ./bin.0
Congratulations! You have successfully executed bin.0 with no input.
```

Run it with arguments:

```
$ ./run.sh ./bin.0 input
Congratulations! You have successfully executed bin.0. Your input was: myinput
```