Secure software development and web security
Homework 2

R. Absil

Academic year 2021 - 2022

This homework requires students to develop attacks related from the third to fifth chapter of the course and, in particular, stack buffer overflow. Note that, for academic reasons, you are not allowed to use decompilation tools.

You will need to set up a linux environment for this project, either booted directed from a drive, or through a virtual machine. You are provided three programs, compiled with GCC with the options

`-m32 -fno-stack-protector -z execstack -g0`.

You will send your results by email, compressed under a `.zip`, `.7z` or `.tar.gz` archive file format. This archive must contain the personal codes you used to answer the following questions, as well as a report under PDF format. The deadline for submission is set on December 5 at 23h59. Failing to meet these demands will result in your homework not being graded.

Question 1 (5 pts)**.** In the binary named "project", there is a secret string hidden[1]. Explain, at least with screenshots, how you recovered it.

Question 2 (3 pts)**.** Consider the `C11` code listed below. This code implement some form of protection against buffer overflow. Explain *two* different ways of bypassing this protection in the particular case of buffer overflow.

```c
int secret; //will be initialised with a random number in the main function

void stuff(char* str)
{
  int guard = secret;

  char buffer[12];
  strcpy(buffer, str);

  if(guard != secret)
  {
    printf("Stack smashing detected. Terminating program.\n");
    exit(1);
  }
}
```

[1] You will know what it is when you find it.

Question 3 (5 pts)**.** In the binary named "check-pwd", find a buffer overflow vulnerability and and how to exploit it to bypass password protection[2].

Question 4 (12 pts)**.** Turn the binary "root-me" into a set-uid program. Find a buffer overflow vulnerability in this program in order to log as root[3].

[2] You will get a bonus point if you also manage to find the password.

[3] Obviously, without providing the root password when running the attack...