PV204 Security Technologies

5th assignment – Reverse Engineering.

Supervisor: Dr.Petr Švenda
Student: Pedro Gomes, 490830

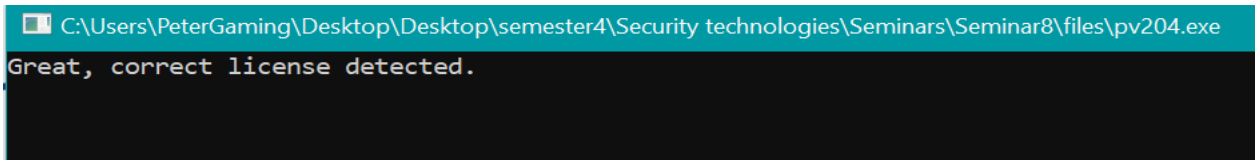
1. Patching

I started by looking in ollydbg where the line that prints the message “Sorry, incorrect license” was. After finding it, I saw where the lines that jumped to it were, and those were the following:

002010F8, 0020112E, 00201133, 002011A1, 002011A3, 002011D8, 002011DA

Starting by the very first address, we can see that it is a line of a conditional jump that comes right after a stream is opened to read some file (the license)

Finally, it was just a question of changing the jump command in: “002010F8” to the address of the line containing the: “Great, correct license detected” message:



2. Creating valid license info

I was not able to create a valid license info. I was only able to detect that the name of the license, should “license.txt”, because that is the name of the file that the binary tries to open.

It is also perhaps possible that the license would require, at least, 8 bytes of data. Probably in ASCII, according to the following:

010c1128 CMP DWORD PTR SS:[EBP-3C],8

This comparison comes after a stream was opened to the license. It is a comparison to the size 8 (bytes).

If the comparison is false, meaning if the license has below 8 bytes of data, the following line is executed:

```
010c112e        JMP 010C11EF
```

Note that “010C11EF” is the line where the *bad boy* is: “Sorry, incorrect license.”