Assignment 3: Software Hijacking

Week 9

Your third assignment is on software hijacking , which is bases on Lab 4. The assignment is an individual assignment and is worth 25% of the module marking. You will be assessed on your ability to carry out a successful exploitation of the software.

Marks Breakdown

5 Marks Decompile the application and figure out:

- **1 Marks: Which function checks the license. (write the function name only)**
- **2 Marks: When this function is run. (Code and explain the sequence)**
- **2 Marks: How the license key is checked? (What makes a valid license?) (Code and explain the sequence)**

5 Marks Generate an unpatched key to enable app (check value). (Flag and explain process)

5 Marks Patch the application to disable online license checks. (Flag and explain process)

5 Marks Patch the application to enable the advanced features. (Flag and explain process)

5 Marks Patch the application to remove reporting metrics. (Code and explain the sequence)

Submission Instructions

Please Submit your solution to this form

Deadline

The assignment deadline is on 13 of May 2021.

Experimental Setup

You will need to use the same Virtual Machine or Vagrant image you used for the previous laboratory.

Download the lab6 application from the following URL: https://git.soton.ac.uk/comp6236/lab6/-/raw/master/lab6-app.zip

Use Ghidra and a hex editor of your choice to reverse engineer the binary and complete the steps above.

You may find the following Assembly instruction reference useful: http://ref.x86asm.net/coder64.html