# Year 10 IST Assignment Two 2021 – Binary Exploitation and Report (40%)

| | Criteria | Mark Range |
|---|---|---|
| Password1 | **Submissions at the top of this mark range will:**<br>• have successfully exploited the binary and determined how the password is validated.<br><br>**A write-up at the top of this mark range will include all the following:**<br>• in-depth, step-by-step detail of the successful exploitation, with reference to breakpoints, memory addresses, and other parts of x32dbg if needed and relevant<br>• discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out.<br>• screen shots at various important steps of the exploitation process. | 5 – 0 |
| Password2 | **Submissions at the top of this mark range will:**<br>• have successfully exploited the binary and determined how the password is validated.<br><br>**A write-up at the top of this mark range will include all the following:**<br>• in-depth, step-by-step detail of the successful exploitation, with reference to breakpoints, memory addresses, and other parts of x32dbg if needed and relevant<br>• discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out.<br>• screen shots at various important steps of the exploitation process. | 5 – 0 |
| SerialKey1 | **Submissions at the top of this mark range will:**<br>• have successfully exploited the binary and determined how it validates the serial number.<br><br>**A write-up at the top of this mark range will include all the following:**<br>• in-depth, step-by-step detail of the successful exploitation, with reference to breakpoints, memory addresses, and other parts of x32dbg if needed and relevant<br>• discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out.<br>• screen shots at various important steps of the exploitation process. | 5 – 0 |
| SerialKey3 | **Submissions at the top of this mark range will:**<br>• have successfully exploited the binary and determined how it validates whether the software should be registered.<br><br>**A write-up at the top of this mark range will include all the following:**<br>• in-depth, step-by-step detail of the successful exploitation, with reference to breakpoints, memory addresses, and other parts of x32dbg if needed and relevant<br>• discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out.<br>• screen shots at various important steps of the exploitation process. | 10 – 0 |
| Challenge | **Submissions at the top of this mark range will:**<br>• have successfully exploited the binary and determined how it determines valid serial numbers.<br>• provide a working keygen to generate valid serial numbers.<br><br>**A write-up at the top of this mark range will include all the following:**<br>• in-depth, step-by-step detail of the successful exploitation, with reference to breakpoints, memory addresses, and other parts of x32dbg if needed and relevant<br>• discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out.<br>• screen shots at various important steps of the exploitation process.<br>• commented code explaining how the keygen works. | 15 – 0 |
| | **In addition, submissions in the top mark range for all activities will:**<br>• use headings to separate out the report into logical sections.<br>• be aesthetically pleasing, with appropriate use of layout techniques.<br>• be readable and easily understandable.<br>• be free of spelling and grammar errors. | |