Year 10 IST Assignment One 2020 – Binary Exploitation and Report (45%)

	Criteria	Mark Range
Password1	**Submissions at the top of this mark range will:** • have successfully exploited the binary and determined how the password is validated. **A write-up at the top of this mark range will include all the following:** • 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 • discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out. • screen shots at various important steps of the exploitation process.	5 – 0
SerialKey1	**Submissions at the top of this mark range will:** • have successfully exploited the binary and determined the correct serial key. **A write-up at the top of this mark range will include all the following:** • 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 • discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out. • screen shots at various important steps of the exploitation process.	5 – 0
SerialKey2	**Submissions at the top of this mark range will:** • have successfully exploited the binary and determined how it validates serial numbers. • provide a working keygen, written as a function, to generate a valid serial number for a given name. **A write-up at the top of this mark range will include all the following:** • 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 • discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out. • screen shots at various important steps of the exploitation process. • commented code explaining how the keygen works.	12 – 0
SerialKey3	**Submissions at the top of this mark range will:** • have successfully exploited the binary and determined how it validates whether the software should be registered. **A write-up at the top of this mark range will include all the following:** • 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 • discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out. • screen shots at various important steps of the exploitation process.	10 – 0
Challenge	**Submissions at the top of this mark range will:** • have successfully exploited the binary and determined how it validates serial numbers. • provide a working keygen, written as a function, to generate a valid serial number for a given name. **A write-up at the top of this mark range will include all the following:** • 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 • discussion of the thought process during the exercise, including rationale for certain decisions and things which were tried but didn't work out. • screen shots at various important steps of the exploitation process. • commented code explaining how the keygen works.	2 – 0
	In addition, submissions in the top mark range for all activities will: • use headings to separate out the report into logical sections. • be aesthetically pleasing, with appropriate use of layout techniques. • be readable and easily understandable. • be free of spelling and grammar errors.	