

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

	Criteria	Mark Range
Password1	<p>Submissions at the top of this mark range will:</p> <ul style="list-style-type: none"> • have successfully exploited the binary and determined how the password is validated. <p>A write-up at the top of this mark range will include all the following:</p> <ul style="list-style-type: none"> • 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
Password2	<p>Submissions at the top of this mark range will:</p> <ul style="list-style-type: none"> • have successfully exploited the binary and determined how the password is validated. <p>A write-up at the top of this mark range will include all the following:</p> <ul style="list-style-type: none"> • 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	<p>Submissions at the top of this mark range will:</p> <ul style="list-style-type: none"> • have successfully exploited the binary and determined how it validates the serial number. <p>A write-up at the top of this mark range will include all the following:</p> <ul style="list-style-type: none"> • 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	<p>Submissions at the top of this mark range will:</p> <ul style="list-style-type: none"> • have successfully exploited the binary and determined how it validates whether the software should be registered. <p>A write-up at the top of this mark range will include all the following:</p> <ul style="list-style-type: none"> • 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
SerialKey3	<p>Submissions at the top of this mark range will:</p> <ul style="list-style-type: none"> • have successfully exploited the binary and determined how it determines valid serial numbers. • provide a working keygen to generate valid serial numbers. <p>A write-up at the top of this mark range will include all the following:</p> <ul style="list-style-type: none"> • 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. 	15 – 0
	<p>In addition, submissions in the top mark range for all activities will:</p> <ul style="list-style-type: none"> • 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. 	