­



**NOVEMBER 2018**

**PRODUCTION**

**LOGBOOK**

**LEVEL 3 EXTENDED PROJECT (2935-03)**

**CANDIDATE RECORD FORM, PRODUCTION LOG AND ASSESSMENT RECORD**

|  |  |
| --- | --- |
| **Candidate’s Full Name:** | Lucian James |
| **City & Guilds Registration Number:** | FBO9891 |
| **Centre Name:** | **Qufaro** |
| **Centre Number:** | **006820** |

**Notice to candidate:** The work you submit for assessment must be your own. If you copy from someone else or allow another candidate to copy from you, or if you cheat in any other way, you may be disqualified.

**To be completed by the candidate**

1. Have you received any help or information from anyone other than you subject teacher/tutor(s) in the production of this work?

Yes No

1. If you have answered yes, give details below and on a separate sheet if necessary.

|  |
| --- |
|  |

1. Any books, leaflets or other materials (e.g. DVDs, software packages, Internet information) used to help you complete this work and not clearly acknowledged in the work itself must be listed below. Presenting materials copied from books or other sources **without acknowledgement** will be regarded as deliberate deception.

|  |
| --- |
|  |

**Candidate’s Declaration:** I have read and understood the above and can confirm that I have produced the attached work without assistance other than that which is acceptable under the scheme of assessment.

Candidate’s Signature: Date:

**Centre Assessor’s Declaration:** I confirm that the candidate’s work was conducted under the conditions laid out by the specification. I have authenticated the candidate’s work and am satisfied that to the best of my knowledge the work produced is solely that of the candidate. Assessment was conducted under the specified conditions and context, and is

valid, authentic, reliable, current and sufficient.

Centre Assessor’s Signature: Date:

**SUBMISSION CHECKLIST**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**Please note:** All elements of the Project are compulsory. Failure to complete or submit an element may result in a mark of zero being awarded.

|  |  |  |
| --- | --- | --- |
| **To include** | **Completed** | **Additional notes** |
| A signed and completed *Candidate record form, production log* and *assessment record* |  | This document. All pages must be completed by the candidate, except for pages 3, 7, 8 and 14 |
| Evidence of the project outcome |  | E.g. photographs of artefact or production; a piece of creative writing (artefact); research based written report; CD/video/DVD of performances or activities; audiotape/multimedia presentation |
| Research based written report |  | If the project outcome is an artefact or a production, **an accompanying research based written report is required** |
| Evidence of a presentation within the production log |  | Presentation on the project process. Where the project outcome is a presentation, a presentation on the project process still has to be completed |

**RECORD OF MARKS**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the supervisor**

Marks must be awarded in accordance with the instructions and criteria in Section 4 of the Qualification Handbook.

Summary information to show how the marks have been awarded should be given in the spaces below in addition to comments in other pages of this document and any supporting information in the form of annotations on the candidate’s work.

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment outcome** | **Max Mark** | **Mark awarded** | **Additional comments** |
| AO1 Manage | 10 |  |  |
| AO2 Use resources | 10 |  |  |
| AO3 Develop and realise | 20 |  |  |
| AO4 Review | 10 |  |  |
| **Total** | **50** |  |  |

**Concluding comments:**

|  |
| --- |
|  |

**Outline details of taught skills:** Record here details of relevant skills taught in a class/group and details of relevant skills taught individually to this candidate as described in the specification. Continue on a separate sheet if necessary.

|  |
| --- |
|  |

**Supervisor’s declaration:** I confirm that no work assessed for the award of the marks above is also to be submitted, or has been submitted, for any other accredited qualification(s).

**Supervisor’s Signature:**   **Date:**

**CONTENTS**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

**Extended Project working title**

|  |
| --- |
|  |

**Planned form of evidence submitted for project**

|  |
| --- |
|  |

This document consists of the pages listed below. Additional journal material, planning evidence, research evidence, presentation evidence, records of meetings with your supervisor and review material may be added.

|  |  |  |
| --- | --- | --- |
| **Page No** | **Title** | **Date Completed** |
| 2 | Candidate declaration |  |
| 3-4 | Submission checklist and Record of marks |  |
| 5 | Contents |  |
| 6 | Record of initial planning |  |
| 7-9 | Project proposal and approval (Part A, B, and C) |  |
| 10 | Planning review (start of project) |  |
| 11 | Mid-project review |  |
| 12 | End-of-project review |  |
| 13 | Summary |  |
| 14-15 | Presentation record (Part A and B) |  |
| 16 | Reflection |  |

Is this extended project part of a group project?

**Yes No**

**Extended Project final title**

|  |
| --- |
|  |

**RECORD OF INITIAL PLANNING**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

**Note:** This section records initial meeting(s) with your supervisor to agree your project proposal.

|  |  |
| --- | --- |
| **Your first idea for topic (to include overall aim)** | The overall aim of the project is to determine the strengths and weaknesses of methods of user authentication individually, and how to use each one optimally. Then make comparisons between different methods to determine which methods are most effective for various use cases.  I plan to individually review methods of user authentication to identify:   * Flaws. (This is very generic… maybe break down more) * Can any of these flaws be resolved? If so how? * Best practices. * How can/should basic implementations of them be improved. * User convenience. * Ease of implementation. * Common attacks.   Then make some comparisons between methods:   * How can each be used and when should they be used? * Should the way we use some methods of user authentication change? * Is there a “best method” ? * Differences in user convenience. * Differences in security. |
| **Your first ideas for research and development of your project** | Identify categories/methods of user authentication, research the basic mechanics of each then research how the basic mechanics can be improved.  Try and include practical primary research as much as possible. Writing actual implementations of a few methods and attacks could be cool, but probably too time consuming to be realistically done for most of them. |
| **Your supervisor’s main comments and advice** | To get a clear idea of the scope you should include what methods you are suggesting.  From the ROIP Advice document : “Rather than talking about ‘research’ in a vague manner you should discuss specific texts and writers that you are going to use as source material. In the same way, rather than just discussing ‘planning’, be clear about exactly what you are going to do next and why. Be specific.” |
| **Changes, clarifications or additions you have made as a result of your discussion with your supervisor** | Making the focus of the project more about passwords, instead of being a “comparison” between a variety of methods, making the scope much more specific.  **Revised topic (including overall aim):**  The overall aim of this project is to determine the strengths and weaknesses of passwords as a means of authentication, and how the strength of password authentication schemes/protocols can be improved to be more resilient to different types of attacks. As well as detailing the workings of these different types of attacks.  I will also make comparisons with alternative forms of authentication such as two factor authentication, which is becoming increasingly common.  This will cover mainly online user authentication due to its great importance to services which are now essential, such as online banking and payments.  **Revised ideas for research and development:**  I plan to first develop an overview of the basic mechanics of password authentication, and its advantages and disadvantages by referring to existing literature.  Then I will research various attacks which can be made to a system which uses password authentication, and ways systems can be made resilient to these attacks. Examples of attacks that can be made are: brute force attacks, Man-In-The-Middle attacks, keylogging.  I will try and include practical primary research as much as possible. Writing actual implementations of systems and attacks could be very interesting but likely very time consuming. |

**Supervisor’s Signature:**  **Date:**

**PROJECT PROPOSAL – PART A**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

|  |  |
| --- | --- |
| **Title of Extended Project** Present the topic to be researched in the form of a short statement/question/hypothesis with clear focus | **How effective are passwords as a means of authentication, how can they be attacked and how can they be made more resilient to attack?**  A quantitative analysis of security is much too complex, so the determined “effectivity” of password authentication will be mostly qualitative. |
| **Provide a brief outline of the research or activity/ task to be carried out and sources to be consulted with** | To determine the effectiveness of passwords as a means of authentication I will review sources such as [1][2][4] to find out information such as:   * How often is security compromised by bad user practices [2][4] * How often is security compromised by bad technical practices * Technical details of password protocols [1]   To see how password authentication systems can be attacked I will review sources such as [5][8]. I will also include primary research when possible, such as investigating the practicality of password hash cracking using Hashcat.  The types of attacks will include:   * reversing captured hashed passwords * social engineering [5] * key-logging malware * Man in the middle attacks * Machine-learning based [8]   To see how password authentication systems can be secured further I will review sources such as [1][3][6][7] to investigate security enhancements such as:   * Multi-factor authentication * Password managers [6] [7] * Improved protocols [1] * Risk based authentication [3]   Some sources I will (probably) use:  [1] [The secure remote password protocol](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.9653&rep=rep1&type=pdf)  [2] [Addressing Misconceptions About Password Security Effectively](https://www.researchgate.net/profile/Peter-Mayer-3/publication/322936260_Addressing_Misconceptions_About_Password_Security_Effectively/links/5b0589ac4585157f87091a2d/Addressing-Misconceptions-About-Password-Security-Effectively.pdf)  [3] [Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild](https://arxiv.org/pdf/2003.07622.pdf)  [[4] Lets Go in for a Closer Look: Observing Passwords in Their Natural Habitat](https://dl.acm.org/doi/pdf/10.1145/3133956.3133973)  [5] [Advanced Social Engineering Attacks](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.683.3165&rep=rep1&type=pdf)  [[6] Password Managers: Attacks and Defenses](https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-silver.pdf)  [[7] Why people (dont) use password managers effectively](https://www.usenix.org/system/files/soups2019-pearman.pdf)  [[8] PassGAN: A Deep Learning Approach for Password Guessing](https://arxiv.org/pdf/1709.00440.pdf) |
| **Provide a brief outline of the course of study or area(s) to which the topic relates** | Module 9 - Identity & Access Management (Authentication, Authorisation & Accountability |
| **Provide a brief outline of any specific resources and/or equipment you may require, as appropriate** | Powerful GPU(s) for practical experimentation with password cracking. (Have access to this, RTX3090, Quadro P5000)  Computing equipment for analysing large password datasets, ideally plenty of ram. (Have access to this) |
| **Provide a brief outline of your proposed action** | Primary research will include:  Analysing/investigating password cracking using hashcat, to understand the practicality of doing so for an attacker.  Analysis of password datasets [such as these](https://github.com/mamatb/OneWordlistToListThemAll).  Reviewing and reading sources and starting the production of the written report will begin in January, and elements of the primary research will be included as the primary research is being done.  Analysis of password datasets would be done first, at the start of February.  Hashcat experimentation would be done after the analysis of the datasets is done, as these datasets are used when performing attacks/cracking passwords (specifically dictionary attacks).  The presentation will be done in April. |

**Candidate declaration:** I confirm that I have read and understood City & Guilds regulations relating to unfair practice as set out in the notice to candidates below.

**Notes to candidates:** You must not submit work which is not your own; lend work to other learners; allow other learners access to, or the use of, your own independently sourced material (this does not mean that you may not lend your books to another learner, but you should be prevented from plagiarising other learners’ research); include work copied directly from books, the internet or other sources without acknowledgement or an attribution; or submit work typed or word processed by a third person without acknowledgement. Failure to comply with these considerations may result in unfair practice and subsequently being disqualified.

**Candidate’s Signature:** **Date:**

**PROJECT PROPOSAL – PART B**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the supervisor**

Please comment below on the validity and feasibility of the proposal (project proposal Part A).

**Supervisor’s comments**

|  |  |
| --- | --- |
| Comment on the clarity and focus of the title chosen | Title is clear and the project focused. |
| Indicate the relation to, and development/extension outside of, the main course(s) of study or interest | OCR A Level Computer Science and Unit 3 of Cambridge Technical Level 3 in IT do both include Cyber Security and briefly mentions password security. This project massively extends the learning from those. |
| Comment on the suitability of the proposed initial sources and research base | The intrusion into password authentication links into “Module 9 - Identity & Access Management (Authentication, Authorisation & Accountability  ”. This project has plenty of research sources available and several are indicated here. |
| Confirm that project is feasible in the proposed timescale and/or indicate any potential difficulties, to include specified resources/equipment | I believe the project can be done well and within the timescale. |
| Outline the scope to produce a project that meets the assessment objectives (**Section 4** of the Qualification Handbook) | I believe that this project has the scope to meet AO1-4 at the highest mark band. |
| Indicate proposed form and date of the presentation | I believe that it is too early to state exactly when the presentation will take place but that it should happen in early April as final submissions for marking will be near the end of April. Generally, students in the past have given a presentation to the class with their supervisor and a small audience of students which is filmed and submitted to the Centre. |

**Indicate the expected format of the project product that will be submitted for assessment**

|  |  |
| --- | --- |
| Written Report | Y |
| Live performance (e.g. music, drama, theatre, substantial presentation) plus written report |  |
| Electronic format (e.g. CD, DVD, video, programme) plus written report |  |
| Artefact (e.g. prototype, model, artwork) plus written report |  |
| Other |  |

**Is this Extended Project part of a group project? Yes No**

**If Yes, identify group members below and confirm that there is a defined Yes No**

**Individual contribution by the candidate.**

**Candidate’s Name:** Lucian James  **Registration Number:**FBO9891

**Supervisor’s Signature**  **Date:**

**PROJECT PROPOSAL – PART C**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**Supervisor’s Full Name: Martyn Eggleton**

**To be completed by the centre coordinator**

Comment on the feasibility and acceptability of the proposal (project proposal parts A and B) as an Extended Project.

**Centre coordinator’s comments:**

|  |
| --- |
|  |

|  |
| --- |
| **Approved** |
| **Approved subject to the implementation of the centre coordinator’s recommendations** |
| **Resubmission required** |

**Coordinator’s Full Name:**

**Coordinator’s Signature:** **Date**:

**PLANNING REVIEW:**

**AT THE START OF YOUR PROJECT**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

This page records your outline plan at the start of your work.

|  |  |
| --- | --- |
| **Outline the steps in your project. You might want to include:**   * What do you want to achieve? * What are your timescales? * What resources will you use? * Who can support you to achieve your objectives? | -The introduction section will be written at the beginning of the project and then rewritten at the end.  -The protocols section needs to be finished by 19/2/22  -Mid-project review 21/2/22  -Analysis of datasets & password cracking analysis needs to be done by 5/3/22.  Collection and compilation of the datasets needs to be done first, this task may be time consuming due to the large size of these datasets.  Powerful computing equipment I have access to at home will be used for these tasks.  Performing this analysis of password cracking and the dictionaries used for password cracking will give me useful information which I can include in the attacks/defences section.  -The attacks section needs to be finished by 19/3/22  -Presentation 28/3/22  -The defences section needs to be finished by 2/4/22  -The conclusion needs to be finished by 16/4/22  This is also the point at which I will probably rewrite the introduction section.  -End of project review needs to be done by 18/4/22  -Project hand in 18/4/22  -Final submission to Qufaro 25/4/22 |
| **Outline any additional advice or comments that you received from your supervisor during this stage** | Whilst writing up your conclusion by the 16th April is just about OK for the 18th April deadline. We need to do the presentations in w/c 28th March and that will need you to have come to the conclusion even if you haven't fully written it up. I would suggest that you move a few dates closer. As it's a little tight at the end. |
| **Outline changes, clarifications or additions you have made as a result of your discussion with your supervisor** | Moved a few deadlines a bit closer.  New outline looks like this:  -The introduction section will be written at the beginning of the project and then rewritten at the end.  -The protocols section needs to be finished by 19/2/22  -Mid-project review 21/2/22  -Analysis of datasets & password cracking analysis needs to be done by 5/3/22.  Collection and compilation of the datasets needs to be done first, this task may be time consuming due to the large size of these datasets.  Powerful computing equipment I have access to at home will be used for these tasks.  Performing this analysis of password cracking and the dictionaries used for password cracking will give me useful information which I can include in the attacks/defences section.  -The attacks section needs to be finished by 19/3/22  -Presentation 28/3/22  -The defences section needs to be finished enough for a presentation by 28/3/22, and 100% fully finished by 16/4/22  -The conclusion needs to be finished enough for a presentation by 28/3/22, and 100% fully finished by 16/4/22  This is also the point at which I will probably rewrite the introduction section.  -End of project review needs to be done by 18/4/22  -Project hand in 18/4/22  -Final submission to Qufaro 25/4/22 |

**Supervisor’s Signature:** **Date:**

**MID-PROJECT REVIEW**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

This page records your outline plan half-way through your work.

|  |  |
| --- | --- |
| **Outline what has been successful and what has been less successful. Have any additions and/or changes been made to your original plan?** | So far, the project is up to date with the plan, I did finish the password protocols section a few days late, but I started the analysis before I finished the protocols section.  I am using a markdown file with version control (whole report has version control) that contains planning information about the project, I am using this file to track major changes to the project and to track my progress.  Successful:  - Finished up the password protocols section mostly on time, with lots of detail.  - Managed to find mostly good quality sources  Not successful:  - Probably not enough sources cited  Changes:  - Renamed “Attacks” section to “Vulnerabilities” and “Defences” to “Mitigations”  - Given password dataset & cracking analysis its own specific section in the report. |
| **Outline your planned steps to complete your project** | - Password dataset & cracking analysis, and then write up that section (started)  - Write up vulnerabilities section  - Write up Solutions section  - Write conclusion  - Rewrite intro & abstract |
| **Outline any additional advice or comments that you received from your supervisor during this stage** | “say in one of the boxes that the changes are just about more appropriate language and that you relaised it was wrong when reading .... or whatever triggered the thought.” |
| **Outline changes, clarifications or additions you have made as a result of your discussion with your supervisor at this stage** | - Renamed “Attacks” section to “Vulnerabilities” and “Defences” to “Mitigations”, as I feel these words are more appropriate. |

**Supervisor’s Signature:**  **Date:**  Prod\_Log\_LJ\_MPR

**END-OF-PROJECT REVIEW**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

This page records the (near) completion of your project product.

|  |  |
| --- | --- |
| **Outline the successes, failures, additions and/or changes you made as you followed the plan in your mid-project review** | ======  **Successful:**  - All sections are completed with at least a reasonable level of detail  - Continued to be able to find good quality sources as I was writing my report  **Failures:**  The practical aspect of my project where I analysed offline password cracking did not work out ideally, this is due to the fact that the set of hashed passwords I sourced from haveibeenpwned was mostly (93+%) identical to one of my password dictionaries, including lots of junk data. This unfortunate lack of quality in my hashed password dataset means I could not reliable make conclusions about the rate at which real-world passwords can be cracked by different password dictionaries.  Falling behind on deadlines since the mid-project review, specifically the presentation was done rather late compared to the original timescales.  **Changes:**  I moved the order of a couple sections around, but aside from that there have not been any other major modifications to the report structure on a high level.  The presentation was not performed in-person like previous planning may have suggested (not sure if it was written down that the presentation would be in-person), instead it was done during a microsoft teams meeting for convienience.  ========  I finished my report in a rather hastily (some may say rushed) manner closer to the final deadline than I would have hoped for, this may have impacted the quality of the report in some ways (I could have covered more vulnerabilities, for example). In the end there wasnt much I could do to resolve this issue aside from work faster near the end of the project.  As mentioned above, the presentation was performed much later than was originally planned as well as being performed differently than originally planned. This was done for increased convienience mainly, but it also means that the video which will be submitted will probably have much better audio quality compared to whatever the setup for in-person presentations was.  The presentation was also longer than I expected (I was going to try and time each section, but I forgot and the presentation went from being 10 minutes to being about 18 minutes), but I don’t think this was a major negative in any way. |
| **Outline any additional advice or comments that you received from your supervisor during this stage** | My supervisor mentioned issues with my Production Log (I’d submitted the wrong version) and the formatting of the evaluation of resources. |
| **Outline changes, clarifications or additions you have made as a result of your discussion with your supervisor in this final stage** |  |

**Supervisor’s Signature:** **Date:**

**SUMMARY**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

This page provides you with an overview of your project.

|  |
| --- |
| **Provide detail of your project title, aims, main content, what you did to achieve your objectives, project findings and conclusions.** |
| Project title: **How effective are passwords as a means of authentication, how can they be attacked and how can they be made more resilient to attack?**  Aims: To investigate the positive and negative aspects of password-based authentication, in the form of the vulnerabilities that such a system may have. This includes investigating the protocols behind password authentication to understand how such systems are secure on a technical cryptographic level.  Main content and findings: I have described a few password authentication protocols in depth, then I proceeded to investigate the vulnerabilities that may exist within password authentication systems. I went into additional depth on the topic of the vulnerabilities resulting from negative user behaviour, especially in their choice of passwords, I did this with a practical investigation using freely available software and data. Once I had finished investigating potential vulnerabilities, I started investigating how those vulnerabilities can be mitigated.  I believe that I have met the majority of, if not all of what I set out to achieve with this project, even if it didn’t happen exactly according to the deadlines I set out. And despite the practical aspect not being as high quality as I would have liked due to low quality data.  I concluded from my project that password-based authentication relies heavily on the knowledge and capabilities of the user. Currently, the main priority for ensuring the security of a system that utilises passwords as a means of authentication should be the education and training of users. |

**Candidate’s Signature:**  **Date:**

**PRESENTATION RECORD – PART A**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

This page records your presentation and its preparation.

|  |  |
| --- | --- |
| **How are you going to present your project?** | A verbal presentation, assisted by notes and slides. |
| **Planned structure of your presentation (e.g. timing, audience, use of visual aids, slides, use of notes, etc.)** | I will try and follow the suggested timing of:   * 1 minute for an introduction * 2 minutes on how I did my research * 4 minutes on the development of the project * 1 minute on the conclusions of the project * 2 minutes evaluating my project   This will then be followed by questions for some amount of time. |
| **Briefly list the main content of your presentation** | - What the project aimed to discover / intro  - How I went about doing research  - How I went about doing the project – good detail about the password cracking analysis.  - What I concluded from my project  - Evaluation of the project |
| **Outline changes, clarifications or additions you made as a result of rehearsal and/or discussion with your supervisor** |  |

**Candidate’s Signature:**  **Date:**

**PRESENTATION RECORD – PART B**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the supervisor**

Record and comment below on the delivery of the presentation

**Supervisor’s record / comments**

|  |  |
| --- | --- |
| **The nature of the audience (include numbers of staff, students and others present)** | 3 students and 1 staff |
| **The nature of the presentation (include use of notes, use of display items, and use of presentation software)** | Done during our usual weekly online meeting due to timing issues caused Sheffield odd Easter Holiday timing. |
| **Comment on the content and delivery of the presentation** | The presentation was excellent, both in terms of content and delivery. |
| **Comment on the response of the candidate to questions that demonstrated understanding and grasp of the project and/or its productions (give examples where appropriate)** | The response to questions showed Lucian knew his subject very deeply. |
| **Outline the nature of any additional evidence that the candidate might add (e.g. speaker notes, hand-outs, presentation slides, recordings)** | The PPT file and recording will be attached. |
| **Proposed date and format of presentation** |  |

**Supervisor’s Signature:**  **Date:**

**REFLECTION**

**Candidate’s Full Name:** Lucian James **City & Guilds Registration Number:** FBO9891

**To be completed by the candidate**

This page records your own evaluation when you have completed your project product and given your presentation.

**Briefly summarise the main learning aims you achieved when completing your project. You might include:**

* New knowledge, skills or expertise that you enjoyed or found valuable
* Strengths and weaknesses of your project
* A consideration of your planning and organisation
* Changes you would make if you carried out a similar project again
* Advice you would give to others undertaking such a project
* Own personal aspirations for further education and career development

|  |
| --- |
| Throughout this project, I have learnt many new things about password based authentication and how to perform research for the production of a written report. I also did some programming for my project, while I didn’t learn many new things doing this programming, it was good practice.  The weaknesses of my project include:   * The unadequate analysis of password cracking utilising the datasets I had gathered, due to low quality hashed password data * Falling behind on planned timescales, resulting in a reasonably significant amount of work having to be done in a shorter amount of time near the end of the project   The strengths of my project include:   * I produced (what I believe to be) good quality explanations of the technical steps taken for password authentication using the CHAP and SRP protocols. * My dataset analysis (not the password cracking analysis) gave me some insight into the password dictionaries that I had collected, and the results from this aligned with my expectations (top2bil-prob most realistic dataset, ASLM least realistic).   My planning and organisation was not particularly good, it wasnt awful but it certainly could have been better. If this was a personal project I wouldnt have done any planning or organisation as I much prefer to get straight into the work.  If I carried out this project (or a very similar one) again, I would have put more effort into sourcing higher quality data for my analysis. This could include attempting to contact authors of related works which collected the data I required to ask if they have it, and if they could share it (probably would not get far, but it would be worth a try).  If I was advising others undertaking an EPQ in cybersecurity, I would certainly advise that time management is considered to be very high priority, additionally I would say that one of the most important things to do is choose a project which you personally have an interest in.  I would like to continue some of the work I started with this EPQ project in some ways, specifically the password cracking analysis, I would be continuing that as a personal project due to the fact that it didn’t work out so well during this project. |

**Candidate’s Signature:**  **Date:**