****

**Project Planning**

**for**

**SEng Malware (SEM)**

**Version 0.2**

**Prepared by:**

1. John Dornheim
2. Chris Durand
3. John Schlatter
4. Shelby Mitchell
5. Alex Lopez
6. Jon Harrity

**CSC 190 Term Project**

**Advisor:** Dr. Scott Jeffreys

Spring 2019

*Made with love in Axinn 806*

**Table of Contents**

1. Requirements Traceability

2. Risk Assessment and Management

3. Quality Assurance Planning

4. Configuration Management

5. Schedule

5.1 Development Schedule

5.2 Testing Schedule

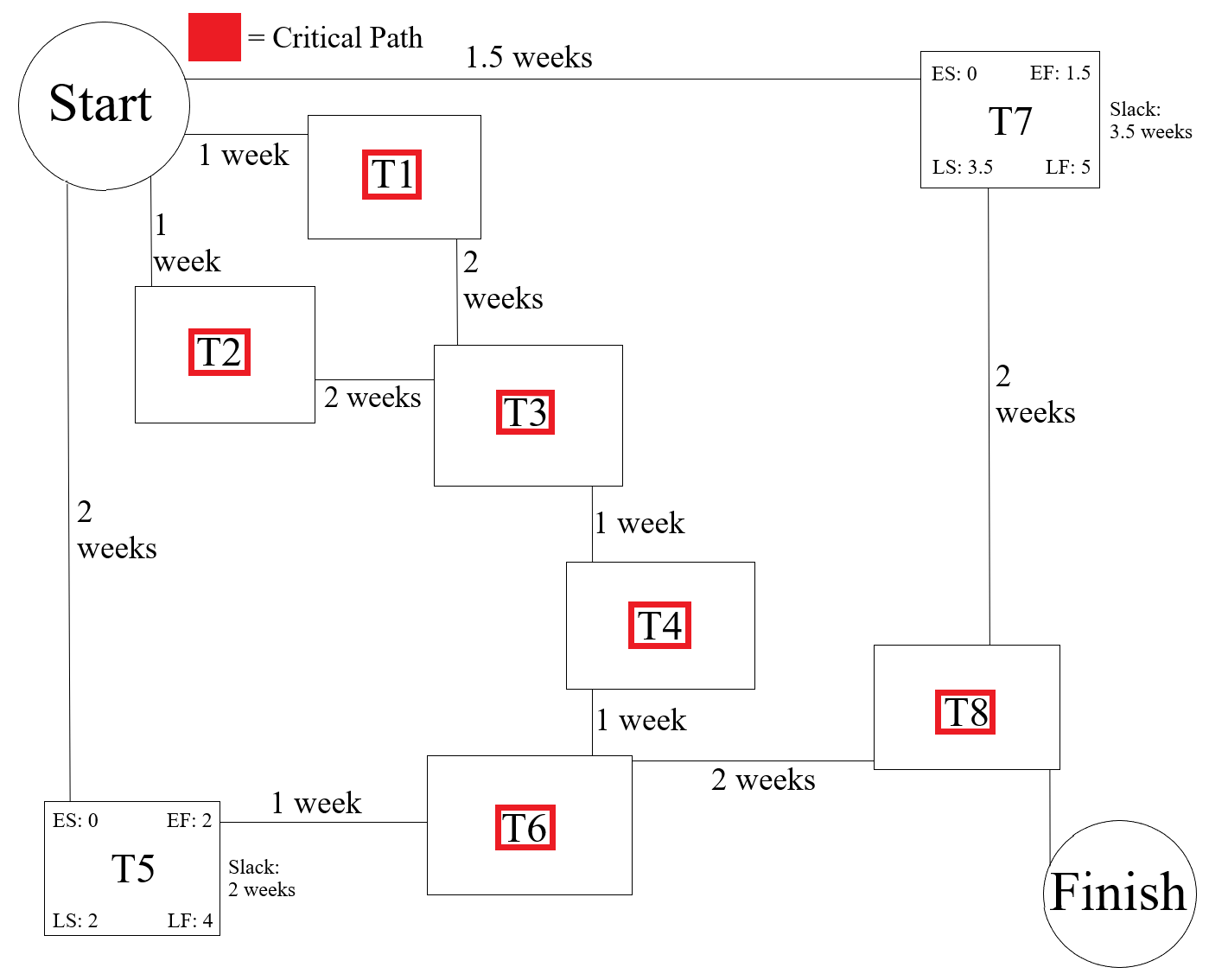
**Requirements Traceability**

Task Dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | TASK | Requirements Point | DURATION (weeks) | DEPENDENCIES |
| T1 | Implementing ClamAV onto Desktop | 4.5, 4.7, 6.2, 7.1.6 | 1 | - |
| T2 | Creating the Deep and Shallow functions to scan a computer | 2.1.1, 3.3, 4.3, 4.4, 4.13, 4.14, 4.15, 7.1.2 | 2 | T1 |
| T3 | Creating UI window for Deep function | 2.1.1, 2.4.3 | 1 | T2 |
| T4 | Creating UI window for Shallow function | 2.1.1, 2.4.3 | 1 | T2 |
| T5 | Creating UI window for Settings | 2.4, 3.1.2(a), 3.1.3 | 1 | T1 |
| T6 | Creating UI window for Logs | 2.3 | 1 | T1 |
| T7 | Creating UI window for Home Screen |  | 1 | - |
| T8 | Linking ClamAV and the UI |  | 2 | T3+T4+T5+T6+T7 |

Critical Path(s):

T1, T3, T4, T6, T8 - 7 Weeks

T2, T3, T4, T6, T8 - 7 Weeks

Slack: T5

Earliest Start: Week 0

Earliest Finish: Week 2

Latest Start: Week 2

Latest Finish: Week 4 T7

Earliest Start: Week 0

Earliest Finish: Week 1.5

Latest Start: Week 3.5

Latest Finish: Week 5

**Risk Management/Likelihood**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Low Likelihood | Medium Likelihood | High Likelihood |
| High Risk | T3 |  | T6 |
| Medium Risk | T1, T4 | T2, T5 |  |
| Low Risk | T7 | T8 |  |

T1 - Risk of not showing all files(hidden files). Can be mitigated by testing to make sure all files are returned and evaluated.

T2 - Limited Experience retrieving and creating file signatures from files. Mitigation

T3 - Limited Experience comparing file signatures. Can be mitigated by focusing on smaller library of malware signatures or on specific types of malware.

T4 - Risk of flagging necessary system-file. Can be mitigated by creating exceptions for the files that we do not want to flag.

T5 - Limited Experience. Can be mitigated by adding more people to task (since this task has slack, can also increase duration needed).

T6 - Risk of components not working together. Can be mitigated by testing each component with expected input/output beforehand

T7 - Risk of user interface not matching the requirements specified. Can be mitigated by referencing requirements during gui build.

T8 - Risk of the UI crashing. Interface misuse. Can be mitigated by thorough testing.

**Quality Assurance Planning**

1. Development Testing
   1. Unit Testing
      1. Guideline Based Testing
         1. T1, T2 - test using list of expected files/signatures to be returned
         2. T4 - test using a list of know files that should be flagged
      2. Partition Testing(Equivalence)
         1. T3- Equivalence classes will be created based off of different types of malware to test.
   2. Component Testing
      1. T6 and T8 - it is important to test the individual components and how they react before linking said components together.
   3. System Testing
      1. Once everything has been linked together, i.e. T8 has been finished, it’s important to test out how the system reacts as a whole independent of how it reacts separately.
   4. Release Testing
      1. Other malware scanner team will prepare test conditions for our system

**Configuration Management**

1. Version Management
   1. Github
      1. <https://github.com/jonharrity/Seng-Malware>
      2. A common git branching model will be followed, as described at <https://nvie.com/posts/a-successful-git-branching-model/> , with the following branches:
         1. Master - Major versions in a production-ready state
         2. Release - branch for new releases
         3. Development - branch for development of the software
         4. Features - a new branch will be made for individual features to the system.
      3. Pull requests will be used for all merges from feature branches to the development branch, for merges from the development branch to the release branch, and for merges from the release branch to the master branch.
2. System Management
   1. ClamAV
      1. ClamAV will be used to assemble program components, data, and libraries. ClamAV is the open source database that houses malware signatures.
3. Change Management
   1. Changes to SEng Malware will be recorded in Github and also by physically logging changes in a separate file for clients’ convenience.
4. Storage Management
   1. The amount of disk space that will be used has yet to be determined.

**Schedules**

**Development Schedules**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Week 1  Feb. 25th - Mar. 4th | Week 2  Mar. 5th - Mar. 11th | Week 3  Mar. 12th -  Mar. 18th | Week 4  Mar. 19th -  Mar. 25th | Week 5  Mar. 26th -  Apr. 1st | Week 6  Apr. 2nd -  Apr. 8th | Week 7  Apr. 9th -  Apr. 15th | Week 8  Apr. 15th -  Apr. 20th |
| Shelby Mitchell |  |  | T3 | T4 | T5 |  |  |  |
| John Dornheim | T1 |  | T3 | T4 | T5 |  |  | T8 |
| Chris Durand | T1 | T2 |  |  | T6 | T7 | T8 | T8 |
| John Schlatter |  |  | T3 | T4 | T5 | T7 |  |  |
| Alex Lopez |  | T2 |  |  | T6 | T7 | T8 | T8 |
| Jon Harrity |  | T2 |  |  | T6 | T7 | T8 | T8 |

**Testing Schedules**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Week 1  Feb. 25th - Mar. 4th | Week 2  Mar. 5th - Mar. 11th | Week 3  Mar. 12th -  Mar. 18th | Week 4  Mar. 19th -  Mar. 25th | Week 5  Mar. 26th -  Apr. 1st | Week 6  Apr. 2nd -  Apr. 8th | Week 7  Apr. 9th -  Apr. 15th | Week 8  Apr. 15th -  Apr. 20th |
| Tasks to be Tested  (end of week) |  | T1 | T2 | T3, T4 |  | T5, T6 | T7 | T8 |