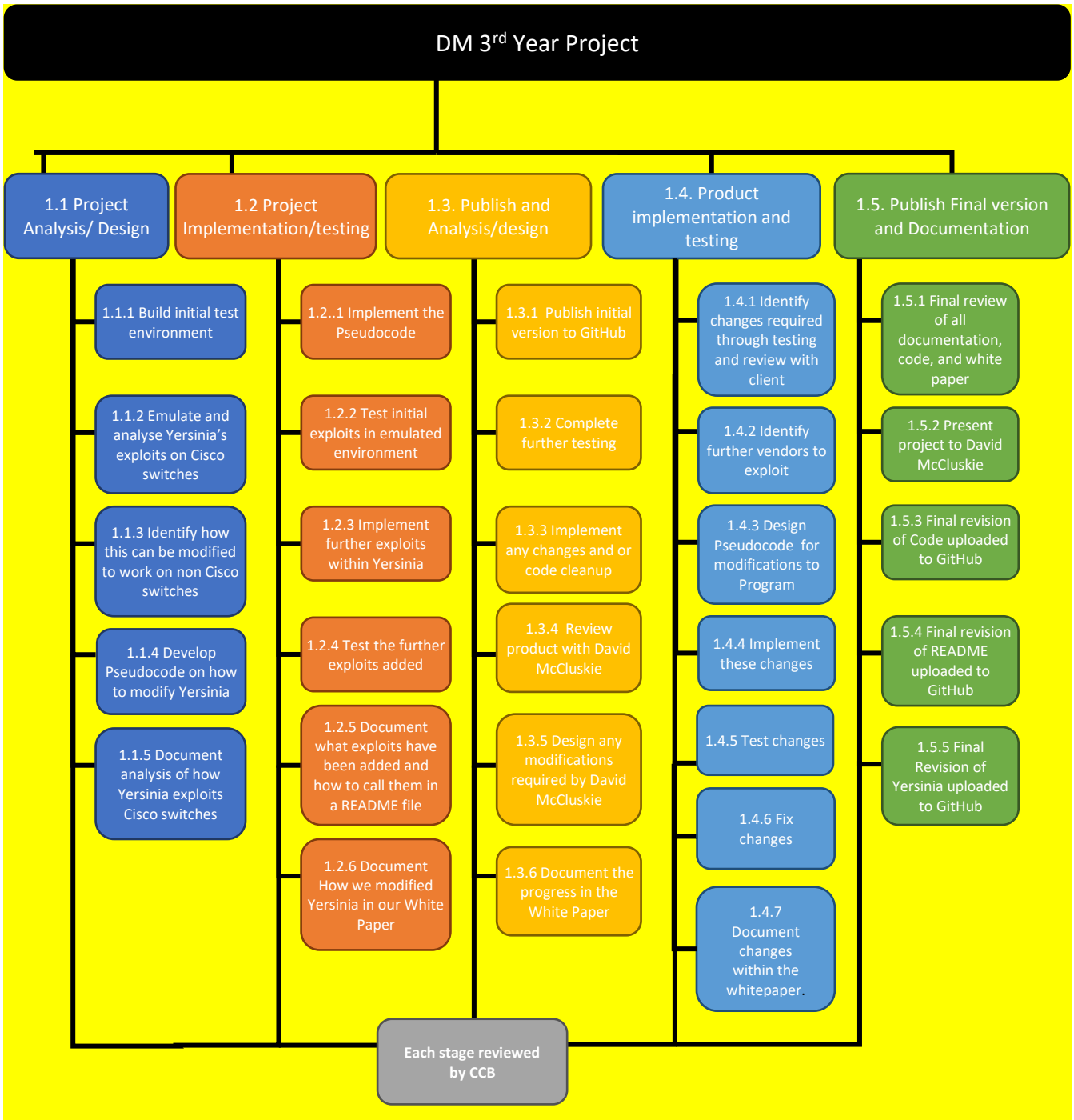
BUSINESS CASE: YERSINIA IMPROVEMENT PROJECT

TEAM ETHICAL HACKING FOUR

Team Member	Sections
PAUL OATES 2001642	9. Introduction 10. Project management approach 11. Project scope and milestone list 12. WBS + Appendix A

ABERTAY UNIVERSITY
DUNDEE, DD1 1HG

DATE: 07.12.22



9. Introduction

As we approach 500 billion connected devices in 2025 (Business Insider, 2015), we see network complexity and size also increase. This leads to more occurrences of vulnerable network equipment that hackers can exploit. To mitigate this, companies employ penetration testers to discover vulnerabilities on their network. Penetration testers are currently limited in their ability to exploit non-Cisco switches, which make up around 21.38% (SL Intel, 2022) of the total market. For this reason, the client David McLuskie has employed our team to improve Yersinia, an open-source tool for exploiting Cisco switches.

The aim of this project is to modify the Yersinia tool so that it can be used to test for security weaknesses with non-Cisco switches. The team Ethical Hacking Group Four will analyse the packets and protocols Yersinia uses to exploit Cisco switches, enabling us to gain an understanding of how Yersinia exploits vulnerabilities in Cisco switches and how this can be modified to work on other vendors. We will modify our GitHub project fork of Yersinia to exploit other switch vendors and release this to the public, we will also produce a white paper documenting our project.

Our project will enable penetration testers to exploit non-Cisco switches allowing for detailed vulnerabilities to be highlighted and resolved. We aim to deliver a modified version of Yersinia freely available for anyone to download on GitHub as well as accompanying documentation. A white paper documenting our processes will be developed for the client. By making use of an Evolutionary (Prototyping) methodology, this will allow us to be flexible and evolve Yersinia into a more thorough pen-testing tool.

10. Project Management Approach

Clear roles for each group member have been devised, this allows for each group member to contribute to the project in a productive manner. Ryan Mudie is our Project Manager and has overall responsibility for the project. This includes: ensuring the project plan is followed correctly and the project is conducted in a timely manner, task delegation, meeting with the client, and any other matters which may arise.

Ryan's primary means of communication with the group is Discord where we have created a group allowing for both live calls with group members and text messages. Another communication method is Microsoft Teams, which has been set up by the University. Ryan can also use the weekly meetings with the group and our project plan on Monday.com to keep up with group members deliverables. In the event that Ryan makes a decision that the group feel is damaging to the project, a vote can be called where a simple majority can overrule Ryan.

The other roles are programmers who include Ellie Macdonald (lead), Ciaran Paterson, and Paul Oates. This group is expected to analyse, modify, document, and produce a test plan for Yersinia. Writers include Amy Agnew, Ryan Mudie, and Suzie McGinness (lead). This group is expected to write the white paper and test the program. The lead programmer, writer and project manager will attend Change Control Board (CCB) a meeting to keep the client updated as the project progresses. Any group issues (writers or programmers) should ideally be resolved within the groups however if no consensus can be met the issue is brought to the Project Manager who will make the final decision.

Any initial funding or upfront costs for software, hardware, training etc will be highlighted to the Project Manager. If deemed necessary, the PM will approach the client for funding and approval. External resources will be identified and sourced during the initial analysis stage such as: firmware from Cisco and non-Cisco switches. The success of the project heavily relies on what vendor switches we can emulate.

Our Group has chosen an Evolutionary (Prototyping) approach as both uncertainty and complexity are high. This allows for prototypes of Yersinia to be shown to the end user through a Change Control Board (CCB) before further refinement. Allowing for the creation of a positive feedback loop, hence making it easier to maintain the project and to meet the clients' requirements. Our chosen methodology also enables the programming group to learn the programming tools and techniques whilst working on the project. This gives the group hands on learning experience whilst developing a meaningful project. As we are not building Yersinia from scratch an evolutionary method of development also allows for us to refine and improve Yersinia into a more capable pen-testing tool.

11. Project Scope and Milestone List

The scope of this project will add the ability to investigate vulnerabilities in non-Cisco switches using Yersinia. No other exploitation tools will be investigated. A white paper will also be delivered to the client. The project does not include a Graphical User Interface (GUI) or a new Cisco exploitation tool and does not include any further maintenance on release. It should also be noted that no outsourcing is required apart from the initial GitHub project fork of Yersinia. The initial analysis stage will determine what vendor switches will be targeted.

The following are the major milestone dates of the project. The major milestones are comprised of a number of smaller tasks.

Emulate Cisco Switch Environment includes - Set up GSN3, Set up appropriate firmware, Analyse Yersinia in Wireshark, Document discovery.

The Project Manager will keep on top of the project with Monday.com any delays identified through the communication management plan which will initially adjust the timeframe. However, if a delay persists the Change Control Board will be notified and will re-evaluate the project scope.

Milestone	Description	Date
Project Start	All resources needed acquired.	30/01/2023
Emulate Cisco Switch Environment	Using software to emulate and analyse how Yersinia exploits Cisco switches	06/02/2023
Complete Initial Yersinia Modification Design	This is an approximate design for the Yersinia modification	13/02/2023
Complete Coding V1	Initial modification to Yersinia complete	20/02/2023
Complete Testing V1	Initial testing to Yersinia complete	27/02/2023
Publish Initial Version to GitHub	Publish forked version of Yersinia	06/03/2023
Identify Further Exploits	Identify further vendor specific exploits to add to Yersinia	13/03/2023
Complete Design V2	Design code for Yersinia	20/03/2023
Complete Coding V2	Complete second code design	27/03/2023
Complete Testing V2	Test modified Yersinia	03/04/2023
Publish Modified Version	Publish	10/04/2023
Consult Project Review Board	The Change Control Board (CCB) will meet to note our progress so far. The CCB can	1/02/2023 08/02/2023 15/02/2023 22/02/2023

	suggest improvements / changes etc	29/02/2023 08/03/2023 15/03/2023 22/03/2023 29/03/2023 05/04/2023 12/04/2023

Our Product and Documentation will be available:

Product	Description	Date
Documentation	Documentation on changes and processes within the project	13/04/2023
White Paper	A white paper documenting or processes	13/04/2023
Modified Yersinia	A modified Yersinia published on GitHub	13/04/2023

12. Work Breakdown Structure (WBS)

The team will work on our project for 1 and a half days per week (12 hours). Our Work Breakdown Structure details tasks as small as 1 hour to 1 day, this enables us to set clear targets. This time allotment has been agreed and approved by all members of our group and aligns with other academic commitments. We will seek approval from the client for the creation of a Change Control Board which will include the client and the writing members of our team, sign off will be recorded at the bottom of this document.

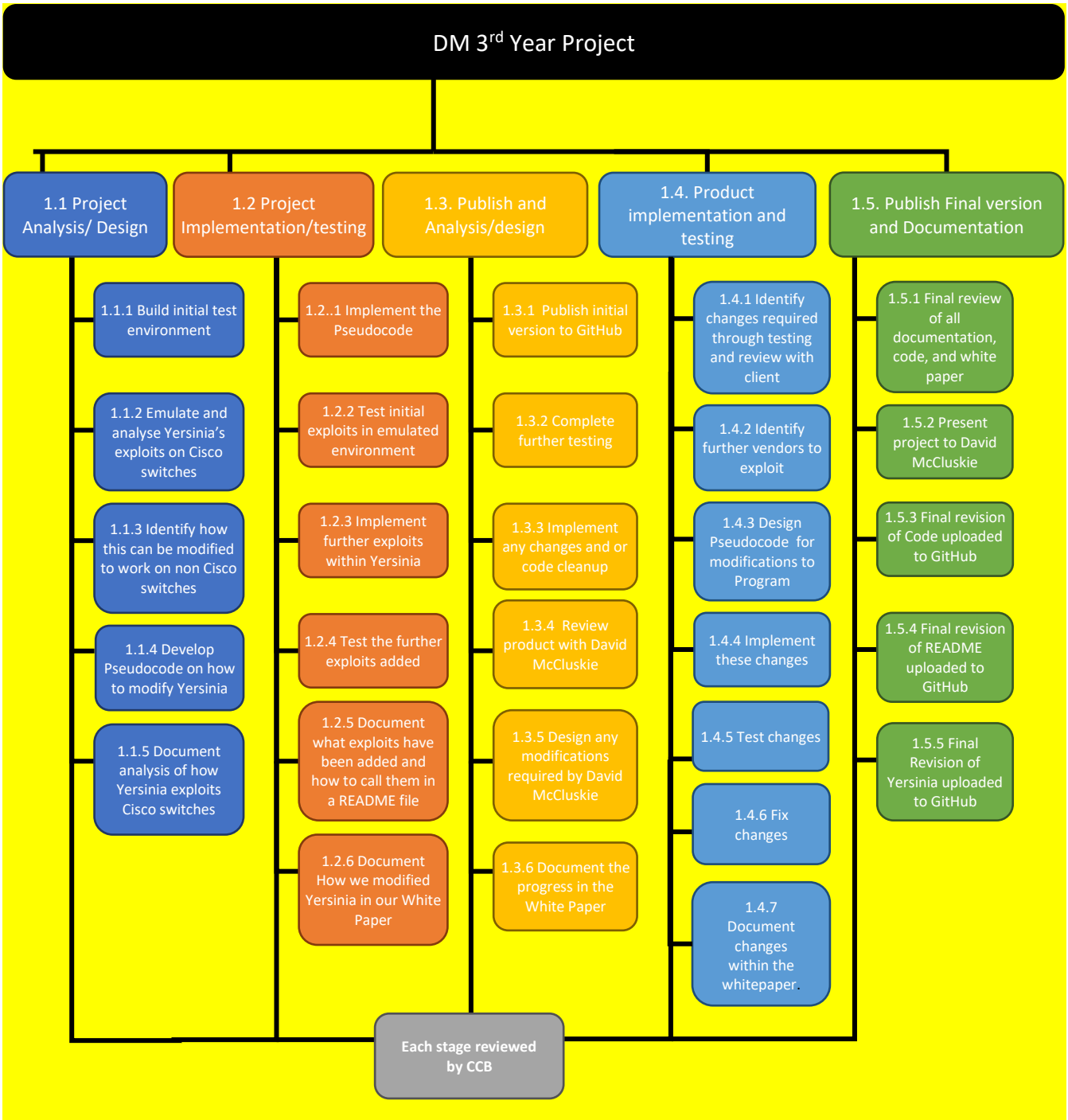
Our Evolutionary (Prototyping) Project Methodology allows for continual review meaning limited impact when changes to the project occur. Regular reviews with the Change Control Board help keep the project on track and within budget. This will also help keep the client updated on the current progress. We will use impact calculations to assess the effect of the proposed changes to the project.

Any required changes in the project will have an impact calculation completed and be brought to Change Control Board for approval.

The WBS found in Appendix A are in the form of a tree structure and tabular table.

APPENDIX A: WORK BREAKDOWN STRUCTURE

A1. Tree Structure



A2. Tabular View

Level 1	Level 2	Level 3
1 DM 3rd Year Project	1.1 Project Analysis/ Design	1.1.1 Build initial test environment 1.1.2 Emulate and analyse Yersinia's exploits on Cisco switches 1.1.3 Identify how this can be modified to work on non-Cisco switches 1.1.4 Develop pseudocode on how to modify Yersinia 1.1.5 Document our analysis of how Yersinia exploits Cisco switches 1.1.6 Consult CCB before moving to next stage
	1.2 Project Implementation/testing	1.2.1 Implement the Pseudocode 1.2.2 Test initial exploits in emulated environment 1.2.3 Implement further exploits within Yersinia 1.2.4 Test the further exploits added 1.2.5 Document what exploits have been added and how to call them in a README file 1.2.6 Document How we have modified Yersinia in our White Paper 1.2.6 Consult CCB before moving to next stage
	1.3. Publish and Analysis/design	1.3.1 Publish this initial version to GitHub 1.3.2 Complete further testing 1.3.3 Implement any changes and or code clean up required 1.3.4 Review product with David McLuskie 1.3.5 Design any modifications required by David McLuskie 1.3.6 Document the progress in the White Paper 1.3.6 Consult CCB before moving to next stage
	1.4. Product implementation and testing	1.4.1 Identify changes required through testing and review with client 1.4.2 Identify further vendors to exploit 1.4.3 Design Pseudocode for modifications to Program 1.4.4 Implement these changes 1.4.5 Test changes 1.4.6 Fix changes 1.4.7 Document changes within the whitepaper. 1.4.6 Consult CCB before moving to next stage
	1.5. Publish finial version and Documentation	1.5.1 Final review of all documentation, code, and white paper 1.5.2 Present project to David McLuskie 1.5.3 Final revision of Code uploaded to GitHub 1.5.4 Final revision of README uploaded to GitHub 1.5.5 Final Revision of Yersinia uploaded to GitHub 1.5.6 Consult CCB before moving to next stage

A3. Glossary

Word	Definition
CCB	Change Control Board. Consisting of Lead Programmer, Writing team and David McLuskie, they will meet after specific stages are met and advise and improve the project
GitHub	A code sharing platform where we will upload our code
Pseudocode	English like language which describes code
Readme	A document with setup / usage instructions
Emulated environment	An environment where we can analyse the packets Yersinia sends
Wireshark	A network packet analysis tool allowing the programmers to understand what packets Yersinia sends
Vendors	Networking companies such as TP-link, D-Link, and Juniper