Kenneth Brown

Kenneth Brown

Tom Neil

Davide Pisanu

Luis Loaysa

Jake Salt

Connor Grattan

Group Project - PMIS

Group 14 - Penetration Testing Scenario

**Contents**

[1 - Project Summary 2](#_Toc64652722)

[2 - Business Case 5](#_Toc64652723)

[3 - Schedule Model 6](#_Toc64652724)

[4 - Configuration Map 7](#_Toc64652725)

[5 – RIC Register 8](#_Toc64652726)

[6 - Client Sign-Off 8](#_Toc64652727)

## 1 - Project Summary

Important Dates

|  |  |  |
| --- | --- | --- |
| Sponsor Appointed | Project Authorized | Project Closed |
| **29th January 2021** | **18th January 2021** | **30th April 2021** |

Purpose

|  |  |
| --- | --- |
| Goal / Outcome | * **To Provide a set of tools and documentation which can be used to create labs for fourth year students to practice security pen-testing in a realistically simulated virtual scenario.** * **To Create one or more scenarios which can be used to test students pen-testing skills in both a logical yet challenging and educational way.** |
| Main product | * **A pre-configured virtual environment or set of environments, which can be used to carry out one or more types of penetration test.** * **An E-commerce style website which is designed for simulating and testing web-based attacks. This will be inside the previously mentioned virtual environment, hosted on a webserver.** * **Documentation that explains each step of all successful pen-tests in a way that they can be easily recreated later for labs.** |
| High-level Requirements | * **Research a variety of pen-testing methods which are used to exploit ‘known’ (or ‘unknown’?) vulnerabilities in a modern OS, Server, web app or software.** * **Documentation which shows these pen-testing methods being used to successfully exploit these vulnerabilities inside a virtual web or OS test scenario.** * **A set of pen-test tools inside a stable, virtual environment that students & demonstrators can use alongside the provided documentation to carry out penetration testing labs.** * **An E-commerce style website that should be used in conjunction with these tools to simulate web-based attacks such as ‘cross-site scripting’ and ‘SQL injections’.** * **Software and hardware used in testing must be of a modern standard to avoid any “out of date” pen-tests which would not be commonly found unpatched anymore in a real security scenario.** |

Targets

|  |  |
| --- | --- |
| Duration | **18th January 2021 – 19th April 2021 (12 Weeks + 2 weeks Easter Holiday)** |
| Budget | **N/A** |

Major Risks

|  |
| --- |
| * **Workflow - At the beginning of the project, when the objectives need to be defined, team members who are dealing with different tasks may have to wait until the previous tasks have been completed to continue. In some cases, this configuration and troubleshooting could become quite time consuming, affecting the project timetable negatively.** * **Experience - Because we are students in these fields, we are immediately at a slight disadvantage. Pen testing against modern hardware and software is generally a task undertaken by professionals with years of experience. Pen testing is one of the harder industry roles to break into because of the layers of knowledge required to discover new vulnerabilities in modern software/hardware.** * **Scope Creep - Project has a large variety of elements to potentially research. Need to keep our efforts in a focused direction to avoid branching out in too many directions, which could harm the quality of the final product.** |

Roles

|  |  |
| --- | --- |
| Sponsor | **Andrew Partridge** |
| Client | **Robert Ludwiniak** |
| Project Manager | **Kenneth Brown** |
| PM Support | **Davide Pisanu** |
| Team Managers | **Tom Neil (Security), Connor Grattan (Web)** |
| Team Members | **Luis Loaysa (Security), Jake Salt (Web)** |
| Supplier PM | **N/A** |
| Consultant/s | **N/A** |

## 2 - Business Case

Purpose

|  |
| --- |
| The business purpose of this project is to ‘***create*** ***penetration testing labs for students’*** which can ‘***improve upon the current standard*** ***of lab being used’*** for teaching within this subject area. The most significant area that needs improvement is with the software versions that the labs currently focus on. Many of the educational labs being used demonstrate pen-testing on *dated* OS versions such as Windows Server 2003, which are no longer commonly found in real world business environments. *As such*, the main goal of the project is focussed on creating penetration tests which can ‘***show exploits and vulnerabilities being demonstrated and taught within a modern OS framework*** **such Windows Server 2016 and above’**. |

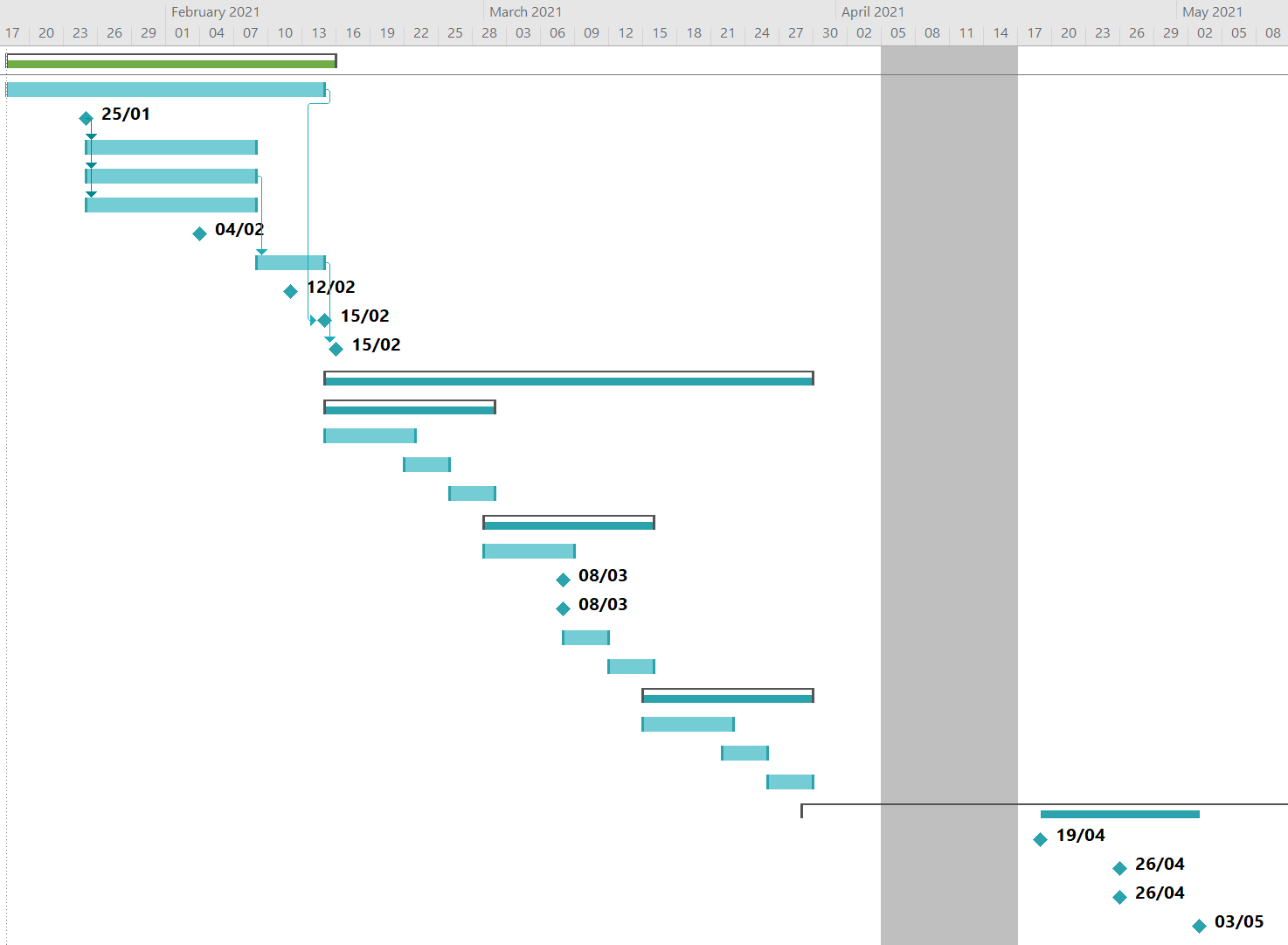
Expected Benefits

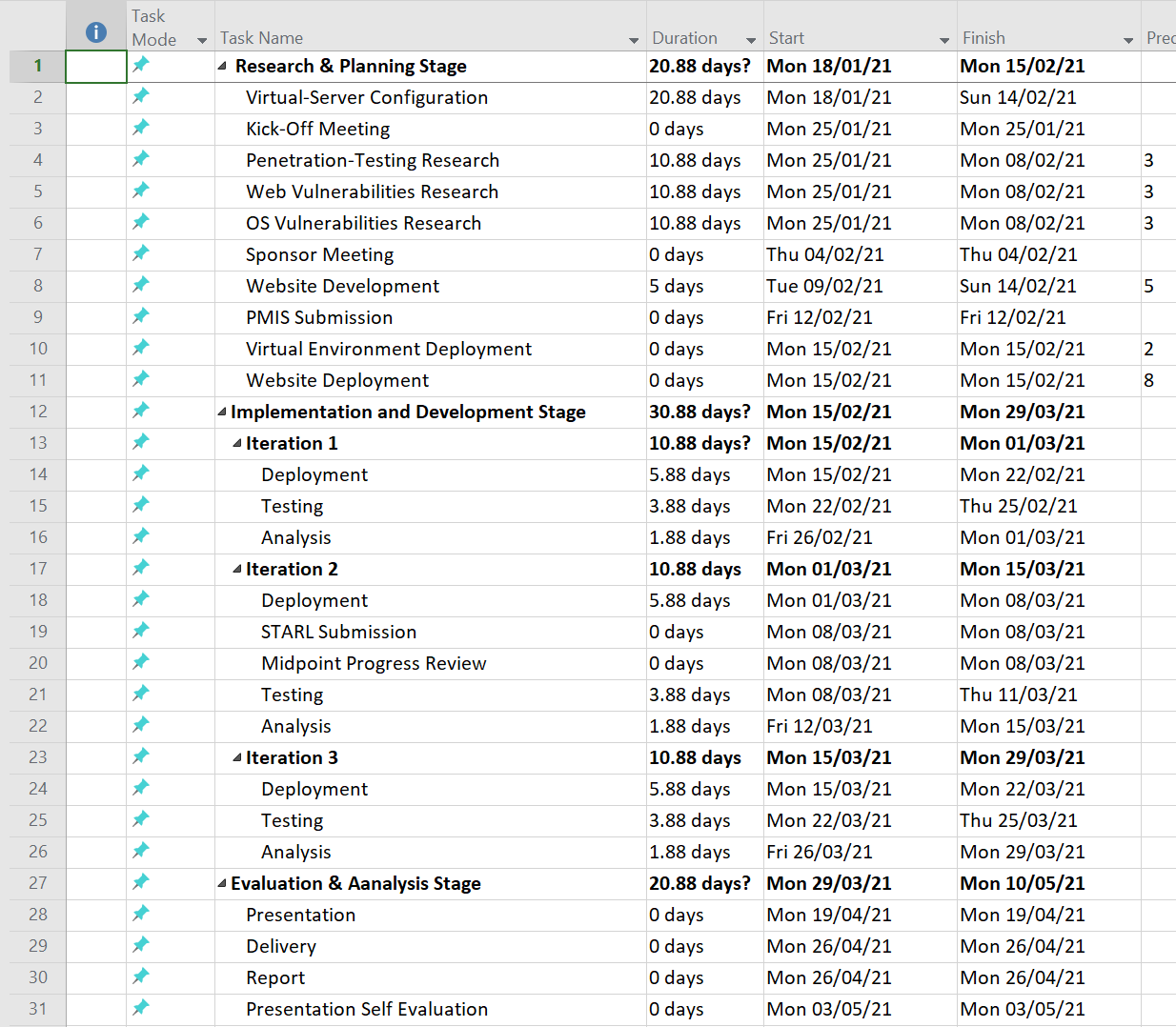
|  |
| --- |
| The main benefits of the project are as follows:   * Students will be able to practice pen-testing on modern OS frameworks, providing a better educational set of tools for real world security scenarios. * Each of the team members are studying related subjects to the project, making this a valuable learning experience for the team itself. * The client should have a wealth of research and documentation at the end of the project from which they will be able to construct more complicated labs for students. |

Expected Dis-Benefits

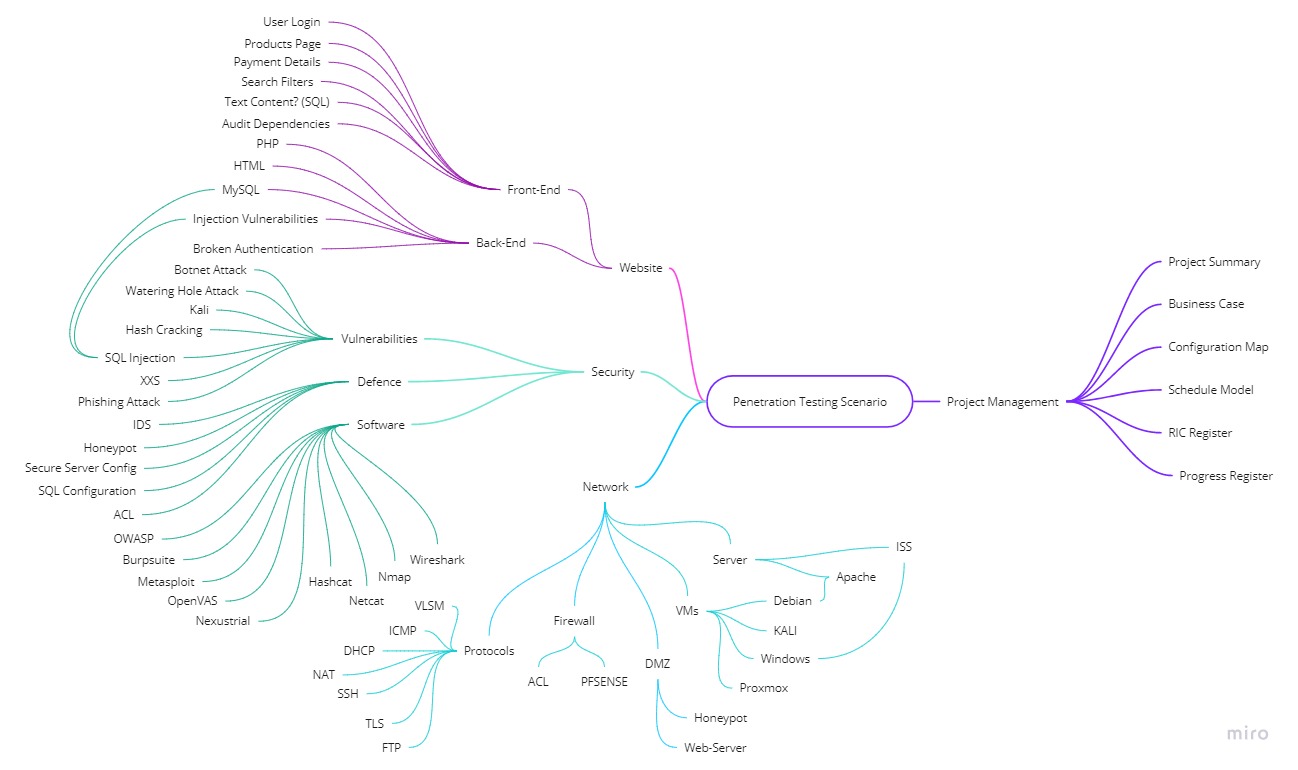
|  |
| --- |
| The main benefits of the project are as follows:   * If the project is not successful in demonstrating pen tests, then it will not be possible to create labs later with the research. * Time constraints may limit the quality of the work that can be produced. |

## 3 - Schedule Model





## 4 - Configuration Map



## 5 – RIC Register



## 6 - Client Sign-Off

Documents checked:

* Project summary
* Business case
* Configuration map
* Schedule model

I confirm that the content of the project management documents listed above provides an accurate and adequate specification of the project requirements.

Signed: Robert Ludwiniak

Date: 15/02/2021