Required Artefacts

Feasibility Demo Project Artefacts – including Gannt chart, Risk analysis, RQ, and Statement on Progress.

Finlay Reid

CMP400: Honours Project

BSc Ethical Hacking Year 4

2021/22

Note that Information contained in this document is for educational purposes.

.

Contents

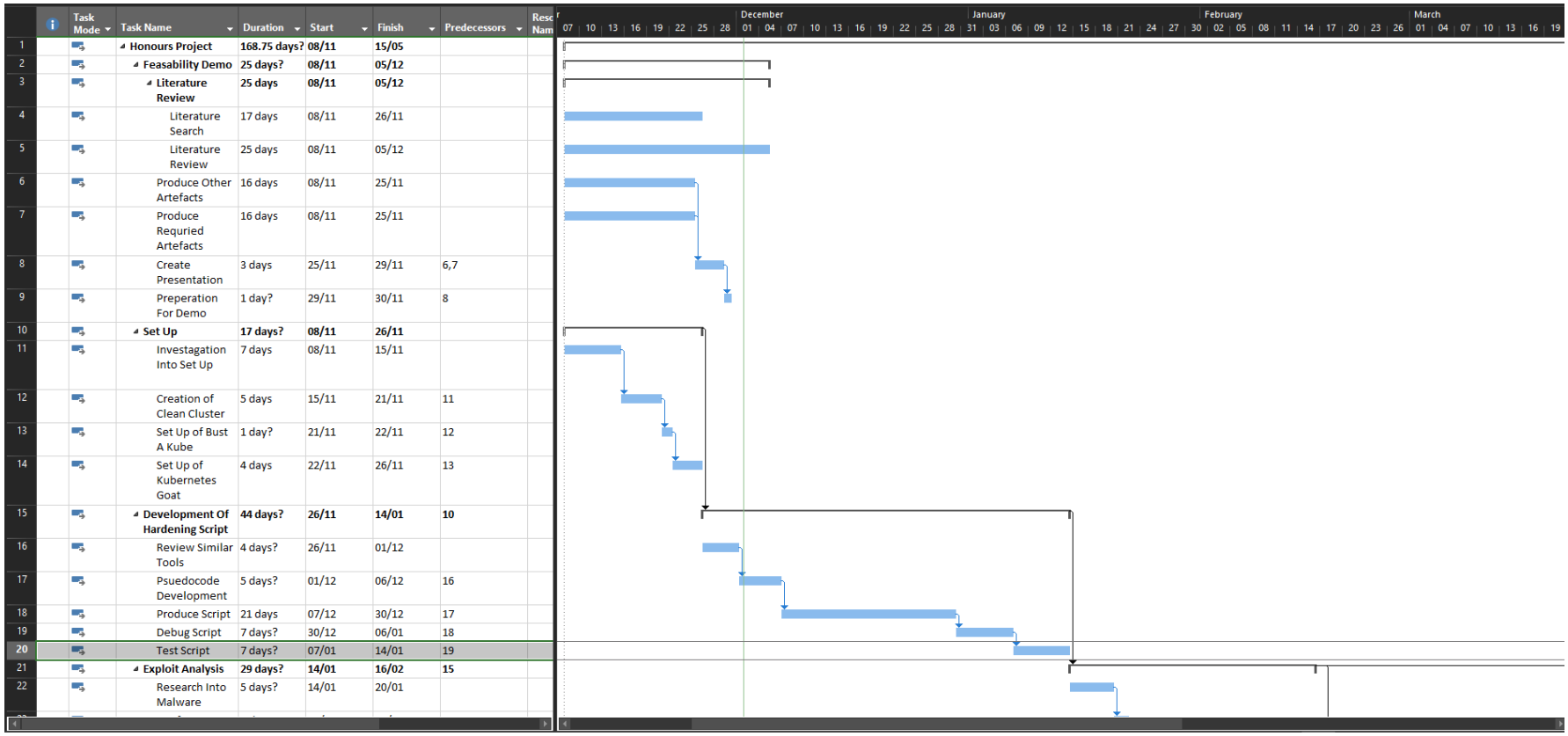
.

1.1 INTRODUCTION

THIS DOCUMENT COLLATES MY REQUIRED ARTEFACTS INTO A SINGLE FILE FOR UPLOAD, THESE ARTEFACTS INCLUDE THE GANNT CHART, RISK ANALYSIS, RQ, AND STATEMENT ON PROGRESS. THE GANNT CHART PRESENTS THE TIME SCALES FOR DIFFERENT DELIVERABLES AND HAS BEEN SECTIONED OFF TO BETTER REFLECT THE DIVERGING OBJECTIVES. TO ENSURE THE RISKS MITIGATION/CONTINGENCY PLANS ARE SUBSTANTIALLY MORE READABLE A TABLE WAS USED TO PRESENT THEM, THIS ALSO DISPLAYS THE VALUES OF THE IMPACT, PROBABILITY AND EXPOSURE WHICH WAS CALCULATED FROM MY INTUITION. THE RISK ANALYSIS IS ALSO PROVIDED IN PARAGRAPH FORMAT. THE FINAL SECTIONS ARE USED TO DESCRIBE THE CHANGES FROM THE PROPOSAL AND THE RESEARCH QUESTION.

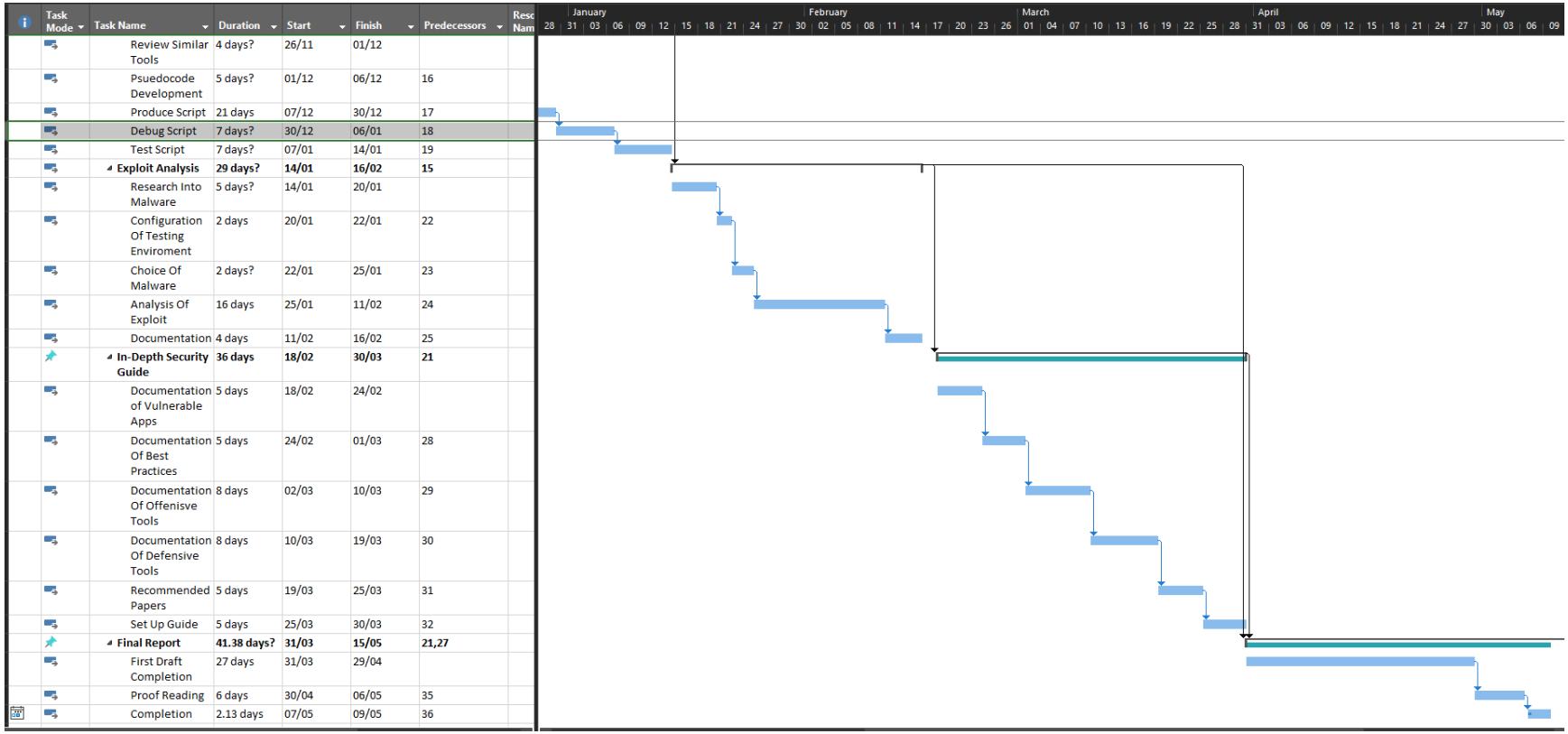
.

2 GANNT CHART



	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		**Honours Project**	**168.75 days?**	**08/11**	**15/05**	
2		**Feasability Demo**	**25 days?**	**08/11**	**05/12**	
3		**Literature Review**	**25 days**	**08/11**	**05/12**	
4		Literature Search	17 days	08/11	26/11	
5		Literature Review	25 days	08/11	05/12	
6		Produce Other Artefacts	16 days	08/11	25/11	
7		Produce Requried Artefacts	16 days	08/11	25/11	
8		Create Presentation	3 days	25/11	29/11	6,7
9		Preperation For Demo	1 day?	29/11	30/11	8
10		**Set Up**	**17 days?**	**08/11**	**26/11**	
11		Investagation Into Set Up	7 days	08/11	15/11	
12		Creation of Clean Cluster	5 days	15/11	21/11	11
13		Set Up of Bust A Kube	1 day?	21/11	22/11	12
14		Set Up of Kubernetes Goat	4 days	22/11	26/11	13
15		**Development Of Hardening Script**	**44 days?**	**26/11**	**14/01**	**10**
16		Review Similar Tools	4 days?	26/11	01/12	
17		Psuedocode Development	5 days?	01/12	06/12	16
18		Produce Script	21 days	07/12	30/12	17
19		Debug Script	7 days?	30/12	06/01	18
20		Test Script	7 days?	07/01	14/01	19
21		**Exploit Analysis**	**29 days?**	**14/01**	**16/02**	**15**
22		Research Into Malware	5 days?	14/01	20/01	

Figure 1 - Gannt chart 1st half



Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resc Nam
	Review Similar Tools	4 days?	26/11	01/12		
	Psuedocode Development	5 days?	01/12	06/12	16	
	Produce Script	21 days	07/12	30/12	17	
	Debug Script	7 days?	30/12	06/01	18	
	Test Script	7 days?	07/01	14/01	19	
	Exploit Analysis	**29 days?**	**14/01**	**16/02**	**15**	
	Research Into Malware	5 days?	14/01	20/01		
	Configuration Of Testing Enviroment	2 days	20/01	22/01	22	
	Choice Of Malware	2 days?	22/01	25/01	23	
	Analysis Of Exploit	16 days	25/01	11/02	24	
	Documentation	4 days	11/02	16/02	25	
	In-Depth Security Guide	**36 days**	**18/02**	**30/03**	**21**	
	Documentation of Vulnerable Apps	5 days	18/02	24/02		
	Documentation Of Best Practices	5 days	24/02	01/03	28	
	Documentation Of Offenisve Tools	8 days	02/03	10/03	29	
	Documentation Of Defensive Tools	8 days	10/03	19/03	30	
	Recommended Papers	5 days	19/03	25/03	31	
	Set Up Guide	5 days	25/03	30/03	32	
	Final Report	**41.38 days?**	**31/03**	**15/05**	**21,27**	
	First Draft Completion	27 days	31/03	29/04		
	Proof Reading	6 days	30/04	06/05	35	
	Completion	2.13 days	07/05	09/05	36	

Figure 2 - Gannt chart 2nd half

3 RISK

3.1 RISK DISCUSSION

Absence due to covid or other illnesses: As the threat posed by contracting covid 19 and other illnesses remains high, necessary precautions will be implemented to ensure the risks are minimized. If a virus such as covid is caught during the project it could significantly disrupt and delay the process, prompting a revision of the project schedule. Mitigation of this risk includes following the guidance set by health professionals, which involves regularly washing hands, wearing a mask, and maintaining social distancing measures. These guidelines will be strictly adhered to ensure the risk of catching covid 19 is mitigated to the highest level. Furthermore, precautions have already been taken to protect against covid 19 as I have received both Pfizer jabs.

Infection of the host machine: Due to the project's investigation into malicious software and the risks these present with a container breakout, there remains a chance of the host machine being compromised. If such a situation arose critical information could be lost, or the home network could be infected comprising other devices. As such necessary steps will be made to ensure this does not occur by collecting the exploits from trusted sources, hardening any virtual machines used within the project, and following security practices recommend by originations when using their software. Having previous experience hardening virtual machines when analysing malware in the mini-project, gives further confidence that the container will be completely secure and isolated.

Getting familiar with new software: The project will require many different components some of which I have little to no experience with. Mostly software-related, as the project relies heavily on the cloud and virtualization technologies. These may include services such as AWS, Kubernetes, and Docker. In order to mitigate the risk posed by this, the research phase of the project will allow me to thoroughly investigate the software which will be utilized in this project. Also, alternative technologies will be explored to ensure there is a backup plan in case a service is unusable. In order to ensure the project runs as smoothly as possible a process model has been implemented for the project. The decision to use the spiral model was heavily influenced by this lack of knowledge pertaining to the software element of the project. A spiral model will enable the project to have many iterations.

Failure of hardware: As the project requires the usual hardware there is a small chance of the machine failing or not being at the level necessary to run the programs needed for the project. Failure of hardware could mean critical files or data relevant to the project might be lost such as word documents, virtual machines, and login credentials for services. If such a situation arose that important data is unrecoverable it would significantly disrupt the project prompting for a revisal of the project schedule. In order to mitigate this risk, necessary steps will be taken including regularly backing up my PC, uploading relevant documents to the cloud, taking snapshots of the virtual machines, and saving login credentials within a password manager. Should hardware issues persist the option to change to a different device is available, for example, a laptop.

.

Scope creep/Gold plating: Gold plating can be defined as implementing new features that were not described within the original project plan, usually additions that barely affect the product. Adding additional features or covering related topics can in theory improve the project but the main functionality will remain the primary focus before addons are considered. Furthermore, any additional features will only be considered if there is a substantial amount of time left before the hand-in date. Scope creep is similar to gold plating and it occurs when the project scope is expanded without consideration of the time constraints. In order to mitigate the risks posed by scope creep the Gannt chart/project schedule will be adhered to rigorously and there will be little deviations.

Overestimation: Due to the ambitiousness of the project, as the final implementation contains several products including an in-depth guide to securing containers, analysis of container and cloud exploits, creation of a script that hardens containers, and a final report. There is a risk that I have overestimated the workload I can complete in the time period given. So as to minimise the risk posed by overestimation the Gannt chart will be strictly adhered to and I will be in constant communication with the supervisor of the project. If I have thought to have overestimated my workload there will be a discussion with my supervisor and we will go from there. There will also be a document created pertaining to the ranking of the different products that will help decide which artifact is to be cut.

3.2 RISK MANAGEMENT MATRIX (RISK EXPOSURE = IMPACT X LIKELIHOOD)

Risk	Impact	Likelihood	Risk exposure	Mitigation plan	Contingent plan
Illness(mental/physical) – through covid or other illness resulting in a delay of the project and therefore straying from the Gannt chart	**9**	**8**	**72**	Follow guidance of health professionals, , remain healthy and take regular breaks.	Rework project schedule, contact project supervisor and take a break until illness has dissipated.
Lack of technical knowledge related to software	**7**	**4**	**28**	Thorough research into software during the research phase of the project,	Allocation of additional research time, Use of backup software.
Infection of host machine – container is broken out and VM is infected	**9**	**3**	**27**	Collection of exploits from trusted data sources and hardening of virtual machines.	Wipe machine, scan using a competent anti-virus, disconnect network.
Failure of hardware – machine fails and the subsequent loss of critical data	8	4	**32**	Regular back of critical data including, snapshots of the virtual machines.	Transferal to new machine and documentation of errors to ensure it does not happen again.
Scope creep/gold plating	**6**	**6**	**36**	Adhere to the Gannt chart, remain focused on primary objectives, add-ons if time is available.	Reconsideration of objectives, reschedule of Gannt chart, and contact supervisor.
Overestimation – overestimating the workload in the given time	**3**	**6**	**18**	Commination with supervisor and strictly adheres to Gannt chart.	Reconsideration of objectives and reschedule of Gannt chart,

.

4 RESEARCH QUESTION/UPDATE OF AIMS

4.1 RQ

What are the most significant issues pertaining to container-based environmental security, and how can these be mitigated through the analysation of exploits, education through a security plan, and the development of a hardening script?

4.2 UPDATE OF AIMS AND OBJECTIVES

<u>Original</u> Aim and objectives:

Aim – The following white paper aims to complete a thorough exanimation of cloud-based environmental security, comparing different hardening methods and discussing the possibility of organizations/users moving to a cloud-based anti-virus instead of local.

Objectives –

- Complete analysis of at least three different techniques used to secure modern cloud environments.
- In-depth review of cloud-based anti-viruses and what one is most effective.
- Display of exploits used to negate the security measures of cloud computing and the possibility of creating my own exploit.

<u>Updated</u> Aim and Objectives:

Aim - The following white paper aims to complete a meticulous examination of container-based environmental security, analyse different hardening methods and assess the risks posed by malicious software.

Objectives –

- Creation of an in-depth container security plan.
- Analysation of container/cloud exploits and their mitigation techniques.
- Discussion of cloud computing's role in containerization and its deployment.
- Creation of script that secures containers.

.

5 STATEMENT ON HOW PROJECT HAS CHANGED

5.1 PROJECT CHANGES

The project has changed slightly, focusing more on container security rather than cloud-based security. However, the cloud will remain relevant to the project, discussing how it relates to containerization.

.

REFERENCES

Mindtools.com. 2021. *Risk Analysis and Risk Management: Evaluating and Managing Risks*. [online] Available at: <https://www.mindtools.com/pages/article/newTMC_07.htm> [Accessed 2 December 2021].

Project-Management.com. 2021. *Tutorial: How to create a Gantt chart in MS project?*. [online] Available at: <https://project-management.com/tutorial-how-to-create-a-gantt-chart-in-ms-project/> [Accessed 2 December 2021].

Rosencrance, L., 2021. *What is Risk Analysis? - Definition from SearchSecurity.com*. [online] SearchSecurity. Available at: <https://www.techtarget.com/searchsecurity/definition/risk-analysis> [Accessed 2 December 2021].

The Writing Center. 2021. *How to Write a Research Question*. [online] Available at: <https://writingcenter.gmu.edu/guides/how-to-write-a-research-question> [Accessed 2 December 2021].