DUY TÂN UNIVERSITY
International School

Capstone Project 1

CMU-CS451

Project Plan Document

Version 1.0

Date: 10/12/2022

Command And Control Attack Simulation & Log Analysis

Submitted by

Pham Anh Khoa

Tran Minh Huy

Nguyen Huy Trung

Tran Van Khoa

Approved by

Tinh, Le Van M.Sc.

Proposal review panel representative

_____

Name Signature Date

Capstone Project 1 – Mentor

_____

Name Signature Date

PROJECT INFORMATION

Project acronym	C2 AS & LA		
Project Title	Command And Control Attack Simulation & Log Analysis		
Start Date	Aug 18th 2022	**End Date**	Dec 10th 2022
Lead Institution	International School, Duy Tan University		
Project Mentor	Le Van Tinh M.Sc. Email: letinh1000@gmail.com Tel: 0935779922		
Scrum master / Project Leader & contact details	Khoa, Pham Anh Email: khosasuke@gmail.com Tel: 0905648553		
Team members	Name	Email	Tel
	Huy, Tran Minh	Minhhuy2015@gmail.com	0935010972
	Trung, Huy Nguyen	huytr.work@gmail.com	0968580247
	Khoa, Tran Van	Tranvankhoa.1998@gmail.com	0522909360

REVISION HISTORY

Version	Date	Updates content	Author	Approval
1.0	Step 3th	Initial Document	Member of C1NE.03	Yes

Table of Contents

1. Introduction

The Project Management Plan will contain the strategy for managing the project and the processes related to all areas of the project, including the project's goals, scope and schedule, information related to staffing, time lines, deadlines, goals and measurements. The plan also serves as a tool for keeping everyone associated with the project on track and focusing on the same details and information.

2. Project summary

2.1. Purpose

The purpose of this document is to guide the development of the project as well as to ensure that the project requirements are in place, the Project Management Plan details the key activities, resources and schedule. Processes and milestones for designing the project and completing the work of the team.

2.2. Project Goals and objectives

The objectives of the project are:

- Perform C2 (Command and Control) attack simulation in detail.
- Design and implement C2 (Command and Control) infrastructure and build and integrate SIEM and projects.
- Recommended to check SIEM software or system monitoring against malicious attacks.

2.3. Scope Definition

The of the project can be summarized as follows:

- Detailed analysis of event information from the terminal.
- Study the techniques involved in malware attacks.
- In-depth analysis of SIEM operations on terminals..
- Design a solution to protect against malicious attacks on endpoints.

3. Roles and Responsibilities

ROLES	RESPONSIBILITIES	PARTICIPANTS
Project Manager	• Schedules meetings, makes sure the meeting process is followed, records result of meeting for future reporting. • Make sure plan is being followed. • Maintain the plan. • Finish assigned tasks.	**Anh Khoa**
Systems Analyst/ Manage documents	• Current status of the monitoring system. • Identify the organizational needs of IT systems. • Research SIEM • Design attack scenarios. • Design defense scenarios. • Research AV engines evasion • Research Tools Hacking	**Anh Khoa,Huy Trung,Van Khoa**
Programmer	• Implement AV bypass techniques on Windows. • Build/deploy C2 and SIEM. • Test system.	Anh Khoa/Minh Huy
Mentor / Coach	• Watches everything, sends obscure signals, makes sure the project stays on course. • Helps with anything.	Van Tinh

Table 1. Roles and responsibilities in capstone 1 project

4. Communication, Tracking and Reporting Plan

The regular reports and communications expected of the project, such as weekly status reports, regular reviews, and as-needed communication. The exact types of communication vary between groups at the start of the project. Specify the reporting mechanisms, report contents, and information flows used to communicate the status of requirements, schedule, budget, quality, risks, and other status indicators both within the project and to external stakeholders. A table such as that below is a convenient way to describe the communication expectations.

Type of Communication	Medium	Frequency	Owner	Audience
Review Status of the Project with the Team.	• Zoom Meeting	Weekly (Saturday)	Project Manager	• Project Team
Update Plan, Tracking Progress	• Dropbox • Google Drive • ClickUp	Weekly	Project Manager	• Project Team
Project Status Report	• Zoom Meeting	Every two weeks	Project Manager	• Mentor • Project Team
Ask, Review Problems	• ClickUp • Zoom Meeting • Zalo Chat	As Needed	Project Team Member	• Mentor • Project Team

Table 2. Communication in capstone 1 project

5. Project Team Information

Name	Contact Email Address	Roles(s)
Tinh, Le Van	letinh1000@gmail.com	Mentor
Khoa, Pham Anh	khosasuke@gmail.com	Project Manager System Analyst Programmer
Tran, Minh Huy	Minhhuy2015@gmail.com	System Analyst
Trung, Huy Nguyen	huytr.work@gmail.com	Manage document
Khoa, Tran Van	Tranvankhoa.1998@gmail.com	Manage documnet

Table 3. Project team information

6. Configuration Management

Configuration Items:

No.	NAME
1	Project Proposal
2	Project Management Plan
3	Project Plan

4	Network Architecture
5	System Implementation
6	Testing Report
8	Capstone source code

Table 4. Configuration items

7. Milestone List

No	Task name	Duration	Start	Finish	Resource
1	**Initial**	**9 days**	**17/08/2022**	**30/08/2022**	**All member**
1.1	Project kick off meeting	5 days	**17/08/2022**	**22/08/2022**	All member
1.2	Discuss about project ideal	2 days	23/08/2022	25/08/2022	All member
1.3	Create Proposal document	2 days	28/08/2022	30/08/2022	All member
2	**Start Up**	**22 days**	3/09/2022	29/10/2022	A.Khoa
2.1	Create Project Plan document	3 days	3/09/2022	06/09/2022	All member
2.2	Create Architecture document	7 days	7/09/2022	14/09/2022	All member
2.3	Create Requirements document	3 days	15/09/2022	18/09/2022	All member
2.4	Create Implement document	1 days	18/09/2022	19/09/2022	All member
2.5	Create Testing document	4 days	19/09/2022	23/09/2022	All member
2.6	Create Design document	5 days	24/10/2022	29/10/2022	All member
2.7	Pre-study	1 days	29/10/2022	30/10/2022	All member
3	**Development**	**28** days	**1/11/2022**	**29/11/2022**	A.Khoa,Huy
3.1	AV engines evasion	14 days	**1/11/2022**	**13/11/2022**	A.Khoa,Huy
3.2	Research VM	2 days	12/11/2022	14/11/2022	A.Khoa,Huy
3.3	Research SIEM	10 days	15/11/2022	25/11/2022	A.Khoa,Huy

3.4	Research Tools Hacking	2 days	25/11/2022	27/11/2022	A.Khoa
3.5	Write Document	1	27/11/2022	28/11/2022	All member
4	**Project's meeting**	**10**	22/11/2022	1/12/2022	All member
5	**Final Release**	**2**	10/12/2022	12/12/2022	All member

No	Task name	Duration (day(s))	Start	Finish	Effort work (hrs.)	Resource Names
1	**Command And Control Attack Simulation & Log Analysis**	**107**	**10/08/2020**	**07/12/2020**	**2675**	**All member**
1.1	**Initial**	**9**	**17/08/2022**	**30/08/2020**	**216**	**All member**
1.1.1	Project Kick Off Meeting	5	17/08/2022	22/08/2022	120	All member
1.1.2	Discuss About Project idea	2	23/08/2022	25/08/2022	48	All member
1.2.3	Create Proposal document	2	28/08/2022	30/08/2022	48	All member
2.1	**Start Up**	**17**	**5/09/2022**	**28/9/2022**	**406**	**All member**
2.1.1	Create Project Plan document	3	3/09/2022	6/09/2022	72	All member
2.1.2	Create Architecture document	7	7/09/2022	14/09/2022	168	All member
2.1.3	Create Requirements document	3	15/09/2022	18/09/2022	72	All member
2.1.4	Create Implement document	2	18/09/2022	19/09/2022	48	All member
2.1.5	Create Testing document	1	19/09/2022	23/09/2022	24	All member
2.1.6	Pre-study	1	29/09/2022	30/09/2022	24	All member

3	**Production Document**	**8**	**3/10/2022**	**21/10/2022**	**312**	**Khoa**
3.1.1.3	Deloyment environment	2	3/10/2022	5/10/2022	48	Huy,V.Khoa
3.1.1.4	Windows Internal	2	5/10/2022	7/10/2022	48	V.Khoa,H.Trung
3.1.1.5	Implement C2 Operations	2	10/10/2022	12/10/2022	48	All member
3.1.1.6	Deloy the attack plan	1	13/10/2022	14/10/2022	24	**Khoa**
3.1.1.8	Testing Document	1	17/10/2022	18/10/2022	45	**Khoa**
3.2	**Design**	**5**	**21/10/2022**	**29/10/2022**	**45**	**Khoa**
3.1.3.1	Design topo C2	1	20/10/2022	21/10/2022	8	All member
3.1.3.2	Deloy C2	1	22/10/2022	23/10/2022	18	All member
3.1.3.4	Topo Defense	1	24/10/2022	25/10/2022	3	All member
3.1.3.5	Deloy Defense	2	26/10/2022	28/10/2022	16	**Khoa**
3.1.4	**Code**	**14**	**1/11/2022**	**29/11/2022**	**672**	**All member**
3.1.4.1	make type struct syscall C++	1	1/11/2022	2/11/2022	24	**Khoa**,Huy
3.1.4.2	Module Stomping	1	2/11/2022	3/11/2022	28	**Khoa**,Huy
3.1.4.3	Queue User APC	2	3/11/2022	5/11/2022	48	**Khoa**
3.1.4.4	Process Hollow	2	5/11/2022	7/11/2022	48	**Khoa**
3.1.4.5	Enum Display Monitors	2	8/11/2022	10/11/2022	50	**Khoa**,Huy

3.1.4.6	Remote Thread Context	1	11/11/2022	12/11/2022	24	**Khoa**
3.1.4.7	Remote Thread Suspend	4	12/11/2022	16/11/2022	96	**Khoa**
3.1.4.8	Current Thread	2	17/11/2022	19/11/2022	48	**Khoa**
3.1.4.9	Sandbox Evasion via Loaded DLL	2	19/11/2022	21/11/2022	49	**Khoa**,Huy
3.1.4.10	Sandbox Evasion via Domain	2	22/11/2022	24/11/2022	10	**Khoa**
3.1.4.11	Sandbox Evasion via User	1	25/11/2022	26/11/2022	25	**Khoa**
3.1.4.12	Sandbox Evasion via HostName	3	26/11/2022	27/11/2022	15	**Khoa**
3.1.4.13	Sandbox Evasion via System Enumeration	1	27/11/2022	28/11/2022	24	**Khoa**
3.1.5	**Testing**	**3**	**27/11/2022**	**30/11/2022**	**75**	**All member**
3.2	**Demo**	**28**	**10/11/2022**	**10/12/2022**	**700**	**All member**

Table 5. Milestone list