CMU-SE450 Capstone Project I

REQUIREMENT DOCUMENT

Command And Control Attack Simulation & Log Analysis

Submitted by

Khoa, Pham Anh
Huy, Tran Minh
Trung, Nguyen Huy
Khoa, Tran Van

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	18– Aug – 2022	**End Date**	10 – Dec – 2022
Lead institution	International School, Duy Tan University		
Project mentor	Le Van Tinh Email: letinh1000@gmail.com Phone: 0935779922		
Partner organization	Duy Tan University		
Project Leader	Khoa, Pham Anh	khosasuke@gmail.com	0905648553
Team members	Trung, Nguyen Huy	huytr.work@gmail.com	0968580247
	Khoa, Tran Van	Tranvankhoa.1998@gmail.com	0522909360
	Huy,Tran Minh	Minhhuy2015@gmail.com	0935010972

REVISION HISTORY

Version	Date	Comments	Author	Approval
1.0	18 Step	Initial Release	C1NE.03 Team	

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Problem

The purpose of this project is to study the execution of a malware attack as well as to simulate the behavior of the malware. With the attack method as well as providing solutions to apply SIEM system to help detect malware risks.

2. GENERAL DESCRIPTION

This project uses C and python for malware development.

Malware development is basically just programming for a very niche purpose, to infect systems. In a red team, this is usually done with the goal of establishing a C2 (Command and Control) session in a target organization.

After completing the software, the deployment of malware attacks with a bug finder meets the requirements of actual drills in the red teams, the rest is for the blue teams to do the deployment. deploy and provide defensive solutions to promptly respond to situations occurring at the enterprise.

The main point of the project is that based on the requirements of the organization owner who wants to test the enterprise's network, it should introduce and apply the SIEM proactive threat detection security model. The SIEM security model promotes a holistic approach to malware infection detection in the pre-deployment phase. To do this, SIEM technologies conduct comprehensive network analysis to detect anomalies.

2.1. Difference Between SIEM and IDS

An Intrusion Detection System (IDS) is a network security technology built for detecting vulnerability exploits against a targeted application. The main difference between a SIEM and IDS is that SIEM tools allow the user to take preventive action against cyber attacks whereas an IDS only detects and reports events.

2.2. Statistics of commonly used bug exploiters

Top Most Prolific C2 Families	
Family	**2020 C2s**
Cobalt Strike	1441
Metasploit	1122
PupyRAT	454

Table 1 : Top detected malware famillies by command and control 2020

2.3. This project have two modules

- User Module.
- Admin Module.

3. STORED PROCEDURE USED IN THIS PROJECT

3.1. User Module

- User can log in to c2 (used for hackers login)
- User disconnect from the current team server
- User Create and edit listensers **Note:** User can change the protocol on the listener (used for hackers create and edit listensers)
- User can view sesion in table
- User can view sesion in graph
- User can create payload
- User can create malicious process

3.2. Admin Module

- Admin login (used for admin login)
- Admin can configure data inputs
- Admin can search data and report
- Admin can create index (admin needs to create archive)
- Admin can save index
- Admin can delete index
- Admin can update index
- Admin can create Forwarding and receiving **Note:** admin will have to forward the OS and get the trace port.
- Admin can update Forwarding and reciving
- Admin can delete Forwarding and reciving.
- Admin can upload file from my computer.
- Admin can view dash board

4. HOW TO RUN SIEM ON THE WEBSITE INTERFACE

Extract the file and copy Downloads folder

Go to the copied path run /opt/Splunk/bin/start

Go to the v4 address and then port 8000 to enter the admin interface.

http://myipaddress:8000

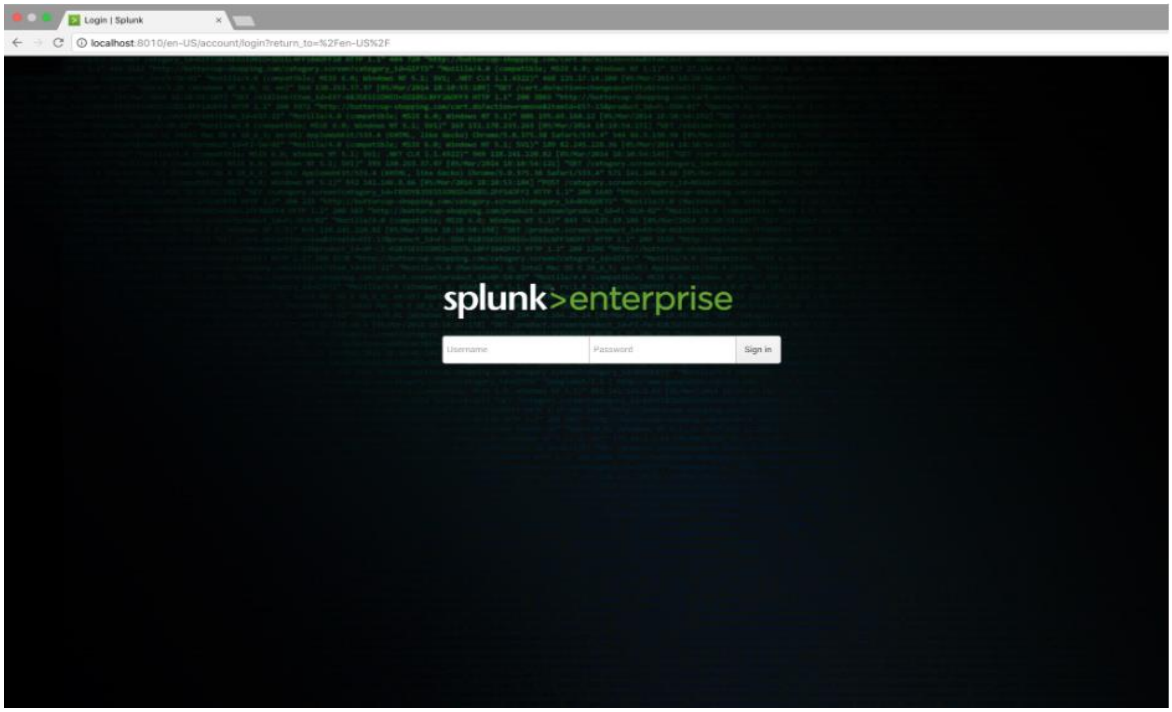

Figure 1 : Splunk Interface Login

5. HOW TO RUN THE USER ON KALI LINUX

Extract the file and copy Downloads folder.

Go to the copied path run ./teamserver <ip_address><password>

Then we need to run the command ./start.sh

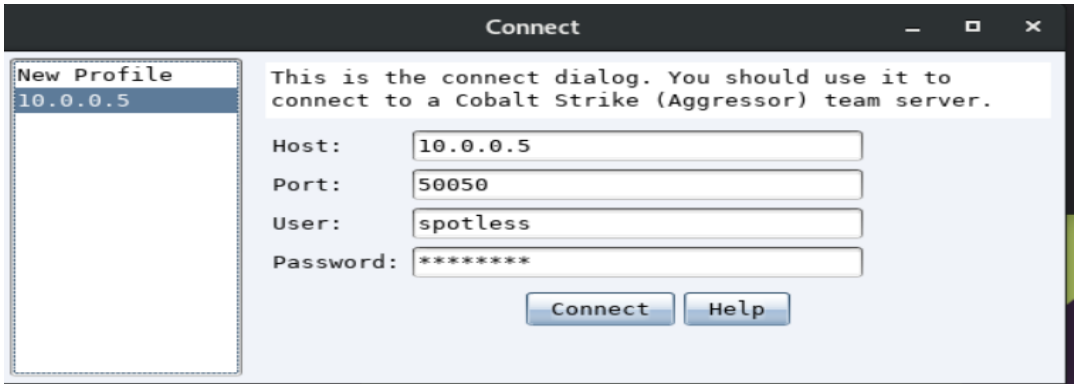

Figure 2 : Cobalt Strike Interface Login

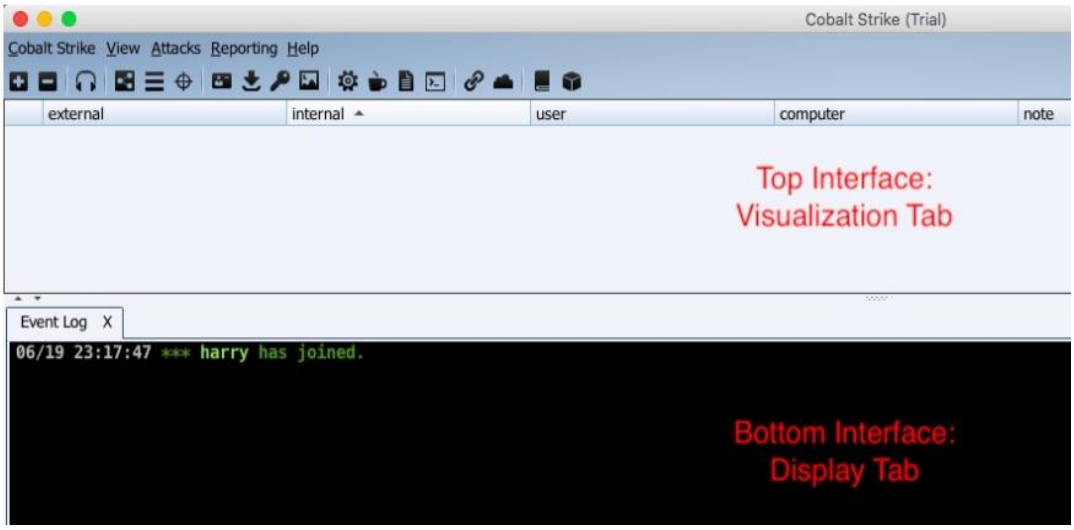

Figure 3 : Main Interface

6. **REFERENCES**

[1] https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/welcome_starting-cs-team-server.htm

[2] https://www.splunk.com/en_us/resources/videos/installing-splunk-enterprise-on-linux.html