Project Deliverable Report (June 2022)

Abstract— This paper will illustrate and describe in detail the deliverables this student had produced and delivered to his industry partner; key decisions and the satisfaction of the project requirements will be discussed in this document as well.

Keywords: Penetration Testing Tools, Hybrid Working Model, Nmap, Wappalyzer, Request, Socket, Subprocess, Argparse, Json.

I. INTRODUCTION

On 15 March 2022, This student had a first meeting with Securestack Company and other intern students, namely Billie Anne Lee, Ler Theng Loo, and Faisal Imtiaz. This student worked 2 days a week in a hybrid working model which means he worked from home using the Gather platform to collaborate with his team members and supervisors on Tuesday and worked at the office on Wednesday.

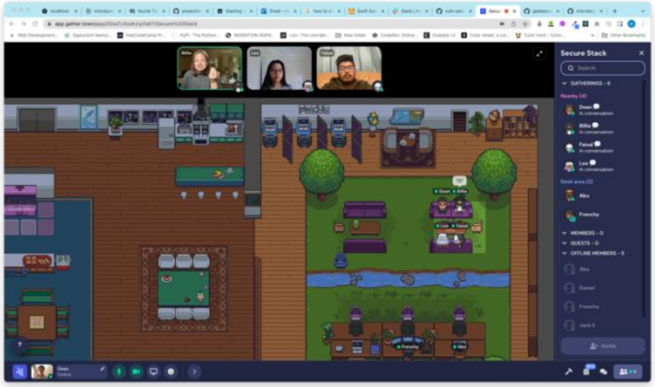

Image 1: Gather Platform was used for online collaboration

II. DELIVERABLE

The main deliverable for this individual student is to build penetration testing tools which allow users to successfully scan websites and get their security test results which include the vulnerabilities. These tools will cover the abilities to:

- Validate the existence of URLs
- Scan websites header and find the security vulnerabilities
- Discover all the technologies and dependencies, such as plugins, programing package libraries, and frameworks
- Scan for websites' trusted certificate
- Spot the physical location of the website server
- Convert scan results to Json format (readable document)

III. DECISION MAKING

A. Initial Decision

To deliver the penetration testing tools on time and align with the project goals that were expected by the industry partner, this student decided to follow:

- Step 1: Learn Bash script (command language), and its penetration testing logic
- Step 2: Convert the penetration testing logic from Bash to Python (programming language)
- Step 3: Learn new Python's package libraries, such as Nmap, Wappalyzer, Request, Socket, Subprocess, Argparse, and Json
- Step 4: Form penetration testing tools using the technologies in step 3

No	Package Libraries	Explanation
1	Nmap	Hosts and ports scanning tool
2	Wappalyzer	Technology Scanning tool
3	Request	Website address's information scanning tool
4	Socket	Network connection tool
C	Subprocess	Run Bash command in Python script
D	Argparse	Convert Python script to command line
E	Json	Convert information to readable format

Table 1: Package Libraries and their usages

This student also decided to use Docker technology, an open platform for developing, shipping, and running applications, in this project. Using the Docker is one of the best practices in software development because it allows other team members to run this student applications on their computing devices without flaws. Before this student started to build actual applications, he used post-it note method to visually his ideas and logic on a whiteboard [1]; then turned it into a Process Mapping as shown in figure 1 and below are the symbols that used in the process mapping:

Symbols	Description
Task	Different functions of the process
Beginning & End Points	Beginning and end points of the process
Inspect & Decision	Places where information is checked against established criteria & decisions made on what to do next

Table 2: Process mapping symbols

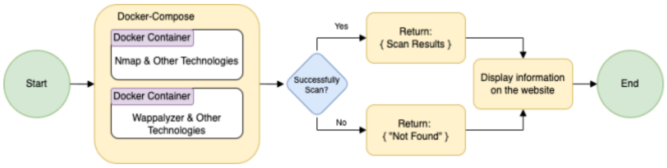

Figure 1: First process mapping (Linear Chart)

B. *Second Decision*

In week 6, a decision was made by the industry partner not to use Nmap and Wappalyzer technologies; instead, a new technology called Nuclei was adopted. Nuclei is a very powerful tool that helps automate vulnerability scanning on web addresses. Since then, this student started working on Nuclei; thus, a new process mapping was created as displayed in figure 2.

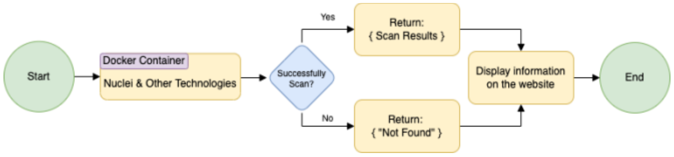

Figure 2: Second process mapping (Linear Chart)

► Finding:

The reason why the industry partner decided to use Nuclei is because it has more Pros than Cons:

Tools	Pros	Cons
Nuclei	Use over 5,000 templates to scan for security vulnerabilities	Take 1 to 5 minutes scan
	Can use a specific template to scan for security vulnerabilities	Not Applicable
	It is a free open source with a large community support	Not Applicable

Table 3: The pros and cons of Nuclei

IV. Satisfaction of Project Requirements

This project was submitted on time and satisfied the project goals. This is because the supervisor supported and mentored this student at each milestone. One to one tutorial was also provided to this student to help him gain an in-depth understanding of what he was supposed to do to complete the project.

The supervisor would check and verify the deliverables at each milestone to make sure that this student was working on the right track; advice would be provided if the deliverables did not meet the requirement.

V. Conclusion

The above sections provide in-depth information on the project deliverables, decision making, and satisfaction of project requirements. As mentioned, this project was delivered on time and verified by the supervisor at each milestone to check the correctness of each task.

References

[1] N. Pearson, E. Larson, and C. Gray, *Project Management in Practice,* 2nd ed. Sydney, NSW, Australia: Mcgraw-Hill, 2019.