**Project Plan and Scope**

**Name BoaPython**

My goal with BoaPython is to create a basic Python tool that automates can automate security-related functions to improve efficiency and security practices. The tool will focus on two key functionalities: vulnerability scanning, log analysis, with a future planned addition of a password management function.

Scope:

With Vulnerability Scanning the plan was to create a function to perform automated vulnerability scanning on target systems that utilize the built-in libraries to interact with target systems. Ultimately reports will be generated on vulnerabilities and security. What we’ll get is a basic vulnerability scan that checks for common vulnerabilities like open ports, old software versions, and poor configurations.

With Log Analysis create a function to analyze log files from various sources while using regular expressions or specific log parsing libraries to extract relevant information. Implements basic analysis techniques to identify suspicious activity and generate a report with findings.

The goal with the addition of password management wil create a function to automate password management tasks like generating strong and random passwords as well as allow users to change or update passwords securely.

**What we should see**

Vulnerability Scanning, Prompt the user to enter a target IP address or hostname.

Perform basic vulnerability checks on the target system, such as scanning for open ports or outdated software versions. Generate Reports

Log Analysis prompts the user to provide the path to a log file for analysis.

Parses log file to extract information, such as IP addresses, timestamps, or error messages.

Basic analysis conducted to identify any suspicious activities or patterns.

Report generated

\*Please note that this is a basic version of the tool, designed so the functionalities and capabilities can be expanded and enhanced based on future projects.