Progress Report 2

Name : Jackie Kim

Student ID : 300376300

Course : CSIS4495-001 Applied Research Project

Description of Work Done

Since the first progress report, I have gathered various tools to develop my automated vulnerability scanning tool. For each tool, I explored its functionality, identified its use in penetration testing, and tested its commands to evaluate whether they produced meaningful and valuable output. After verifying the commands, I developed a Python script to execute them all at once and generate a report.

As I continued exploring more tools—including Nmap, OpenVAS, Metasploit, Nikto, Xprobe2, SMBClient, WhatWeb, and Hydra—I spent significant time debugging my script. Eventually, I realized that combining multiple tools into a single script introduced errors due to differences in their output formats, increasing the complexity and likelihood of failures.

After discussing my project with Priya, I recognized that my initial approach was too vague. I needed to clearly define my end user, the purpose of the project, the expected outcome, and the specific type of scanning I was conducting. This reflection helped me refine my project scope and ultimate goal. I decided to focus specifically on network security scanning and web application security scanning.

Following my consultation with Priya, I finalized my toolset, choosing Nmap for network security scanning and Nikto for web application security scanning. I systematically explored and tested various commands for these tools to maximize the quality of the output and finalized the set of commands to be executed by my automated penetration testing tool.

To enhance the analysis, I sought to integrate an AI tool that could process the scan results and suggest remediation methods. Initially, I attempted to use LangChain but encountered issues because it required a paid API key for analysis. After further exploration, I discovered Ollama, which suited my needs better. I then began integrating it into my existing script.

Repo Check-In of Implementation Completed

In the "Misc" folder, the file "JackieK_WorkLog.xml" contains my work log, which includes a detailed breakdown of the hours spent and a comprehensive description of the research conducted.

Within the "Misc/codes" folder, multiple versions of the scripts I developed are stored.

- pentesting.py and pentesting2.py are scripts without AI integration.
- pentesting_langchain.py incorporates the AI tool LangChain.
- pentesting_ollama.py integrates the AI tool Ollama.

The "Misc/commands" folder contains files documenting the command lists I explored. These files also include screenshots of the output generated by each command.

Lastly, the "Misc/output" folder holds samples of the generated output from my automated penetration testing tool.

Work Log

Date	Number of Hours	Description of Work Done
25-Feb-25	1.5	Researched about AI tool for remediation suggestion
26-Feb-25	4	Tried to integrate LangChain (RAG AI tool) with existing code
28-Feb-25	4	Explored more tools and commands (Masscan, tcpdump, netcat, sn1per)
01-Mar-25	6	Explored more tools and commands (Arachni, burpsuite, commix, dirbuster, dnsmap, sublist3r, openVAS, hydra)
02-Mar-25	4	Explored more tools and commands (little bit more on commix, fierce, Dirb, WPScan, ettercap, xsser)
03-Mar-25	4	Finalized the commands which will be used for scanning and developed python scripts
06-Mar-25	1	Based on the conversation with Priya, the end user, the scope of scanning, its purpose, and the final deliverable were clearly defined, making the objectives more specific and well-defined.
08-Mar-25	6	Continue developing automated scanning tools and AI integration. Decided to eliminate using Semgrep tool. Simulated environment for testing purpose was established.
09-Mar-25	4	Struggled with integrating AI tool. It seems like there is problem with API key for AI tool.
11-Mar-25	3	Changed AI tool from Langchain to Ollama since langchain tool requires API key. Worked on python script to integrate new AI tool
12-Mar-25	6	Finalized Network Security Scanning Tool : Nmap, Web App Security Scanning Tool : OWASP ZAP. Another verification for OWASP ZAP is required. If this can not be verified, I need select second best tool.
14-Mar-25	4	Changed web app security scanning tool : nikto, tested Ollama tool for analysis report.
16-Mar-25	4	Generated AI integrated script, generated progress report