Progress Report 1

Name : Jackie Kim

Student ID : 300376300

Course : CSIS4495-001 Applied Research Project

Description of Work Done

In this progress report, I have conducted extensive research on the planning and scoping phases of penetration testing. I thoroughly explored each step of penetration testing, detailing the importance of every stage and identifying key tasks that need to be performed. The research also focused on reconnaissance, particularly in the context of white-box testing, where I defined and elaborated on the concepts of passive and active reconnaissance, highlighting the objectives and significance of each. I investigated the tools used during the reconnaissance phase, ensuring that I could identify which tools would be most effective for gathering the necessary information in a white-box testing scenario. Furthermore, I delved into the scanning and enumeration phase, identifying the critical components to be scanned and the risks each poses to an organization. This research will serve as a foundation for building an automated penetration testing tool, as it has allowed me to define essential tasks, select appropriate tools, and understand what vulnerabilities and components should be scanned.

Throughout the process, I encountered a few challenges related to synthesizing the vast amounts of technical information into clear and actionable steps. To address these challenges, I broke down the research into manageable tasks, focusing on each phase of penetration testing individually. This allowed me to make more sense of the complex material and organize the research logically.

Repo Check-In of Implementation Completed

In the "Misc" folder, the file "JackieK_WorkLog.xml" contains my work log, which includes a breakdown of the hours spent and a detailed description of the research conducted. Additionally, the file "Research Contents for Pen Testing Procedure," also located in the "Misc" folder, contains the organized research information described in the work done section of this report. This document outlines the details of the research on reconnaissance, the scanning and enumeration phases, and includes citations and references for proper documentation. It also highlights potential risks related to scanning and enumeration. Additionally, under the "ReportsAndDocuments" folder, this progress report will be uploaded as "JackieK_ProgressReport1.pdf."

Work Log

Date	Number of Hours	Description of Work Done
16-Jan-25	2	Researched the background of penetration testing (steps, methods, types, etc.) and gathered the necessary information.
18-Jan-25	2	Studied the methods of penetration testing
19-Jan-25	2	Created bold outline of the research design, objectives, methodology and its justification
20-Jan-25	3	Make plans for the research timeline and generated the proposal draft
23-Jan-25	2	Updated proposal and submitted
27-Jan-25	1.5	Researched detailed information about planning and scoping in penetration testing
29-Jan-25	2	Gathered the information about planning nad scoping and generated step by step report
31-Jan-25	1.5	Researched detailed tasks and background information about reconnaissance
03-Feb-25	2	Gathered the information about reconnissance in penetration testing and updated detailed tasks decription. Researched tools can be utilized for reconnaissance.
05-Feb-25	1.5	Researched bold outline of scanning and enumeration phase of penetration testing. Identified components can be scanned and the importance(risks) of those components.
07-Feb-25	3	Researched which tools can be used for each scanning strategy
08-Feb-25	1	Progress Report 1 was generated