Flaw Hypothesis Methodology-Based Project

The Goal

A group with members here at UC Davis and at NAI Labs have developed a specification-based method for detecting and handling intrusions. (You will learn about all this later.) They have implemented their techniques on a web server running on a target system. They believe the techniques make the web server very hard to degrade or crash, and protect the system from intrusions (and crashes) originating at the web server.

The goal of this penetration study is to attack the web server. You want to achieve any of the following goals:

- Crash the web server;
- Crash the system; or
- Obtain access to the system underlying the web server.

Note that you are *not* to attack the system itself directly. The system is *not* hardened against attack (although the project members have taken prudent steps to protect it).

The Project

Ifyou choose to do this project, you must use the Flaw Hypothesis Methodology to analyze the security of the web server on this system. In particular, you will need to analyze the server. You will *not* have access to the underlying system, so must use information from the server's replies to figure out what the server is. From that, and from other information you gather (if any), you must hypothesize weaknesses, design tests, carry out the tests, and generalize the results.

Requirements for the parts of this project are below.

Part I: Project Selection

Submit the required template for part 1. In your paragraph, describe how you will document your work using the Flaw Hypothesis Methodology. In particular, how will you record your hypotheses, tests, and results? How will you describe your generalizations?

Part II: Project Design

At this point, the information gathering phase should be complete, and you should be generating hypotheses about flaws. You will need to present the information you have gathered and derived, and list several hypothesized flaws, as well as ways to test them.

Part III: Completed Project

For this part, you need to submit the information gathered, your hypothesized flaws, your priority of testing for them, the tests and results for any flaws you tested, and generalizations. Each test should be described separately, and in enough detail to allow us to perform the tests and have the same results.

Important Note

If you decide to do this project, you will be ***required*** to attack the web server from a specific system. This will prevent you from being identified as a malicious attacker who needs to be reported! I will have accounts created for all students working on the project, and will give those students the host name and IP address after the accounts are created.