HACQIT Project Part 3

Introduction

Phase 2 required you to probe the systems on the HACQIT enclave. The next phase asks you to exploit the information you gathered.

What is Due

Please try So do your best, and—as always—show a typescript (for example, from *script*(1))

1. Identify 5 known vulnerabilities for the weaker version of IIS on the HACQIT cluster. Can you find any vulnerability for the stronger version of IIS? Identify one or more CGI script vulnerabilities for both Apache and IIS web servers in the cluster. Find exploits for two different types of vulnerabilities that you believe will work against at least one of the web servers in the cluster. Why do you believe they will work against the cluster? How do they work? What objective, result or capability do the exploits enable you to achieve?
2. Run the exploits for your vulnerabilities against the HACQIT protected web server. What is the effect? Are you able to gain Administrator privileges or crash the web server? Since multiple teams share the login server, how do you know it was your exploit that caused the effect? Does either exploit work more than once?
3. *Extra credit*. Develop your own exploit for a known vulnerability in IIS. Test the new exploit against the cluster. Submit the exploit with explanation of how it works and what it enables you to do.

For each vulnerability you find, and each exploit you try, you must create a notebook entry. This "notebook" is virtual (put the entries into a file and submit them using *handin*, as usual). This format follows the Flaw Hypothesis Methodology, which we discussed in class. (If you need to review it, please see section 19.2.4.)

Due Date

This is due on Friday, March 15, at 5PM.

Notebook Entry Format

Each entry consists of 3parts. They are:

1. *Hypothesis*. What vulnerability are you testing for, and why do you believe it exists in the target? Your hypothesis may be based upon specific characteristics of the target (such as running a particular server), upon knowledge of the operating system (such as it being MonsterOS 3.8, and MonsterOS 3.8 is known to have this vulnerability in its TCP/IP stack), or upon knowledge of the system (such as looking at the source to SDNS, and seeing a vulnerability in it). Please state clearly what you suspect the vulnerability is, and why. Provide any general information about the target that helped you decide that this particular vulnerability might exist.
2. *Testing*. State how you will test for the vulnerability, and carry out the test. You can use soneone else's code for the test, but you must make sure it runs, and explain why the program/routine you are using does in fact test the vulnerability. (You have to be specific about your test. You *cannot* say that "I found Tony's attack tool for this vulnerability at attacks-r-us.com." You need to show how the tool works, and why it will establish whether the vulnerability exists.)
3. *Generalization*. If your test fails, why did it fail? Are similar tests likely to fail also? Should you look for other types of vulnerabilities? If your test succeeds, what other vulnerabilities similar to this one might exist? Why do you think so?

It is perfectly fair for you to turn in 4 related vulnerabilities. For example, one vulnerability may lead you to a generalization that suggests other vulnerabilities. If this happens, *please* document your thinking in part 3, and name the files containing the suggested entries.