10–2–14 CSE 4243/6243 Homework 2 - Working With Vulnerabilities

Introduction

An important part of most security-related work, both offensive and defensive, is the ability to analyze published information about new vulnerabilities. When defending systems, it's important to be aware of patches and workarounds that prevent systems from being compromised. When attacking systems, it's important to be able to quickly understand how a vulnerability works, so that an exploit can be developed and used effectively.

In this lab, you are to create a report that represents the research you will be performing on the recently-disclosed vulnerability in Bash, which has been nicknamed "Shellshock" by the information security industry. I am intentionally not providing any more information than is necessary to uniquely identify the vulnerability in question. The purpose of this assignment is to exercise your ability to find, understand, and act on vulnerability information.

Your report should present information about the "Shellshock" vulnerability in a professional manner suitable for a target audience of fellow vulnerability researchers that, while savvy on terminology and technology, do not necessarily have prior in-depth knowledge of the vulnerable software or the vulnerability in question. This assignment provides a set of topics that must be discussed for full credit, though your report should not be structured in typical "homework", "question and answer" style. Instead, the report should address those topics in a whitepaper-like style meant to be read by professional.

While you are responsible for determining the structure and formatting of your report, you are to work within the following requirements:

- There should be a title page
- You are required to have the following sections, in addition to the sections you will add to address the required topics
  - Introduction
  - Conclusions
  - Bibliography (or References)

Required Topics

You are expected to address the following topics in your own words, and support statements that you make with the sources you have found in your research:

- Discuss the purpose of the Bash software. What is its normal usage? How is it used by other software?

- What public vulnerability databases have information on this specific vulnerability? What identifiers (names, numbers, etc.) have been assigned to this vulnerability by these databases?
- Who discovered the vulnerability? Where was it originally published? Is there any information about how disclosure was made to the Bash developers?
- Describe the vulnerability in technical detail, to include, but not limited to: Is it a design problem, or a coding error? What portion of the software is vulnerable, and why does it represent a security problem? Your description of the vulnerability should be detailed enough for a peer to understand the bug well enough to understand it and exploit it without referring to your source material.
- How can one determine if a particular installation of Bash is vulnerable? If you find code or commands that accomplish this task, describe what each portion of that code or command is doing.
- Describe how the vulnerability in the code was patched. Was there more than one attempt at patching the vulnerability? If so, what was insufficient about earlier patches?
- Describe two real-world scenarios in which this vulnerability can be exploited to gain remote command execution on a vulnerable target system. How does other software interact with Bash in a way that allows for remote exploitation of this vulnerability?
- In a virtual machine or the lab environment, demonstrate the exploitation of this bug:
  - Set up a target system with a vulnerable version of Bash and whatever other software is needed to create the vulnerable environment.
  - Exploit the target system, demonstrating that you can gain remote command execution on that system.
  - You may write your own exploit code, or use exploit code from the Internet. You are required to discuss how the exploit works in enough detail that another programmer could replicate it without access to the original code.
  - Document this process with screenshots and descriptive text that would allow another vulnerability analyst to replicate/verify your work.

Deliverables

Your submission should be in the form of a compressed .ZIP file that contains your report in PDF format, as well as any code or scripts that you used in the demonstration of exploiting the vulnerability. This is to be submitted via MyCourses in the “Submit Assignments” section of the course. This assignment’s due date/time is 9:30AM on Tuesday, October 14th. The late penalty for homework assignments is described in the syllabus.

Academic Integrity

Homework assignments in this class are strictly individual work. Do not discuss any aspect of this assignment with fellow students. Assignments will be checked for evidence of plagiarism. Use and cite resources appropriately.

Grading *(points for not following instructions taken off of the grade determined by this scheme)*

- 10% - Spelling, grammar, appropriate technical writing style. Avoid conversational/ informal tone.
  - All students are encouraged to seek (and acknowledge) writing and proofreading assistance from one of the university's writing centers.
- 10% - Professional formatting, organization of your document
- 10% - Quality of required sections, *Introduction* and *Conclusions*
- 30% - Demonstrated exploitation (last set of bullet points in *Required Topics*)
- 40% - Remainder of the *Required Topics*