Network Security Project

Instructor: Shiuh-Pyng Shieh
Email: TA@dsns.cs.nycu.edu.tw

1. Warning

Please be aware that **Plagiarism is not permitted**. TAs will do a plagiarism check at the end of the semester. If caught plagiarizing, it will result in a failing grade for the course.

2. Project Description

The goal of this project is to reproduce the CVE vulnerability environment and exploit it. Finally, find the corresponding log in the system.

3. Project Guide

I. **CVE Vulnerability**: Select a CVE vulnerability from the list we provided on E3 platform.

II. **Environment**: For those CVE vulnerabilities that may require a specific environment or version, you need to set up your own virtual machine or docker on your computer.

III. **Exploitation**: You need to describe what you did to exploit the vulnerability step by step and what code and tools you used. If you have any references to any writeups or bug reports, please cite and briefly describe the related work.

IV. **Log**: You need to find the corresponding log in the system. We will specify software that collects the log for each OS.

4. What to Submit

I. A report

A report containing:

1. CVE vulnerability introduction.
2. How you reproduced the CVE environment.
3. How you prepare to reproduce the exploitation.

II. The code for reproduction and explanation

1. The code that you implemented or open-source code for reproducing the CVE vulnerability and exploitation. You need to encapsulate your code into a single script or an executable file.
2. Append your explanation into the original report submitted in the first phase.

III. The corresponding log/mitigation and explanation

1. Each CVE requires a submission of a screenshot of the results.
   - CVE-2023-4357:
     i. Content of host-dependent file (e.g., /etc/passwd) and terminal for opening file server.
     ii. Additional Requirement: Feasible mitigation and reasons for their feasibility.
   - CVE-2023-38545:
     i. Capture the screenshot of sock5h proxy server during the attack, the terminal to execute exposure, and the result of exposure.
     ii. Find the corresponding log based on the specific log-

collecting software.

- CVE-2023-44487:
  i. Find and filter important network flow by Wireshark and find the corresponding log based on the specific log-collecting software.
  ii. The screenshots should include the filtered network flow, the terminal while executing exposure, log relative to your attack, and the experiment result.

2. Append your explanation into the original report submitted in the second phase.

5. How to Submit

I. The report
- Due Date: 3/26
- Upload the pdf to the e3 platform

II. The code and the second version report
- Due Date: 4/23
- Upload the updated pdf to the e3 platform
- Upload the "<student_number.zip>" file containing the code
  - The structure needs to be:
    <student_number>
    |- <student_number>.pdf
    |- code

III. The log and the third version report
- Due Date: 5/28
- The corresponding log
- Upload the updated pdf to the e3 platform