

CSCM28: Security Vulnerabilities and Penetration Testing

Coursework 2

Phillip James

Due: 11:00am, 25th March 2020

This coursework involves demonstrating a security vulnerability, showing how the vulnerability can be exploited on a technical level and demonstrating how the vulnerability can be patched.

You should produce a software based demonstrator for the vulnerability you chose to explore in Coursework 1. This demonstrator should contain the vulnerability you documented and allow you to illustrate an exploitation of this vulnerability. You should also then demonstrate a patch for this vulnerability that causes your exploit to fail, or demonstrate/discuss why a patch is not possible.

You will be expected to give a short demonstration (up to 10 minutes) of your solution in the week following the submission deadline. You will also be expected to submit the underlying source code with details of how to run the exploit. The coursework will be marked against the following criteria:

Presentation

- Overview of system setup and explanation of vulnerability. [4 marks]
- Clarity of demonstration of exploit. [4 marks]
- Demonstration of patch, and exploitation failure. [2 marks]
- Overall level of technical discussion and response to questions. [4 marks]

Submission

- Relative ease of setup, i.e. are all required libraries packaged with the submission. [3 marks]
- Quality and clarity of README file. [3 marks]

Marking

This task will be marked out of 20 marks based on the above rubric. The overall mark will be calculated as a combination of a mark achieved from presenting your demonstrator along with marks from the quality of the submitted demonstrator. The presentation will take place in the week following the submission deadline.

Submission

You should submit a zip file via Blackboard containing both your source code and instructions on how to setup and run your demonstrator. If your source code is larger than 200MB (e.g. because it is a virtual machine image) then you should provide a suitable link for downloading your software (e.g. a GitHub link). Your instructions for running the demonstrator should be including in a README.txt file and should include details on how to setup the system, run the exploit and then patch the exploit.

Submit your work via Blackboard before **11:00am, 25th March 2020**.