FAF.CS16.1 Fall 2020

Lab 4: Enforcing a Policy

Handed out: Tuesday, September 22, 2020
Due: Tuesday, September 29, 2020 (20:15)

Introduction

In this course you will do a sequence of labs, the end goal of which is to develop a Security Benchmarking Tool (SBT). These labs will familiarize you with instruments used in IT security departments of different companies as well as give you practical experience in developing them. Concretely, you will be working with cyber security audit policies – benchmarks that allow a security officer to assess a system's vulnerability to different attacks and enforce certain security configurations based on community best practices.

Enforcing a Policy

Following the audit results, a user comes to the conclusion that their workstation is misconfigured. In this lab, you will implement features that would allow a user to enforce a policy on settings that are not set according to said policy. After showing the audit results on screen, your application must allow the user to select some, or all, tests that have the status "Failed". After selection, the user should be able to enforce the selected settings, meaning your program will change the settings according to the guidelines specified in the audit policy. Lastly, the program should provide a way to rollback to the system's initial settings, if the user decides they do not like the new ones. To summarize, your application must enable the user to:

- Select the settings to be enforced (a subset of "Failed", or all of them);
- Enforce the policy on at least 5 settings (edit the selected settings in your system);
- Rollback to the system's initial settings.

Reporting

At the end of this lab, you will need to present your source code and a screen recording of the functionality that you have implemented. The links to your video and source code must be uploaded on Moodle, in the Submit Lab 4 assignment activity. Don't forget to make your code public on any hosting service of your choosing (e.g. Github, Bitbucket etc.). Any code on Github must contain a *readme* file (here's a tutorial on how to make a good one).

Grading

At the end of this lab you are expected to provide an application that would contain the features described in the previous chapter, alongside all features described in previous labs. Showing working features in a terminal or a GUI with only a subset of features and placeholder buttons is also acceptable, for a penalty. However, be aware that you'll still need to implement whatever you skipped for the following labs. What is not acceptable is *not providing anything on the day of the deadline*, so don't do that.

Future labs

In the following labs you will implement features that would allow the user to enforce a policy on *all settings* that failed the audit test i.e. are not set according to said policy.

Good Luck!