FAF.CS16.1 Fall 2021

Lab 3: Auditing a Workstation

Handed out: Friday, September 24, 2021
Due: Friday, October 01, 2021(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.

Auditing a Workstation

After importing an audit policy, parsing it and selecting a subset of options, it is finally time to check the system for weaknesses. In this lab, you will implement features that would allow a user to audit their workstation and output the result on screen. The audit must compare the values of different computer settings with values or intervals specified in the policy. If the system setting complies with policy values, the test is considered passed. If not, however, the test should output the value specified in the settings together with the policy values, so that the user can see what is the mismatch. The output of an audit scan should consist of a list of tests and their statuses: "Passed" or "Failed" (and "Reason", where applicable). To summarize, your application must enable the user to:

- Perform an audit of the workstation, using the options that were selected;
- Output the results of the audit on screen.

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 3 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 the policy on settings that are not set according to the policy.

Good Luck!