Hostscan exercise

Jens Schønberg

April 2022

1 Exercise 1. Lynix, simple scanning

This exercises just uses the simple self-contained Lynis scanning tool. There are more elaborate and complex tools available, such as vulnerability scannings tools, for instance:

- OpenVAS

- Nessus

- Vuln

- quite a few more ...

Here we'll be using https://github.com/CISOfy/lynis

1. git clone the project

2. cd into it

3. run sh ./lynis audit system

4. running with sudo will yeild more

2 Exercise 2. Scanning using Yara

Going through a simple example, just to show how to use the basic rule set. In the exercise, try installing yara if you haven't already, and then creating some basic fules set for a simple program. Try playing around, you can also try some modules.