LWASP

Linux Watchful Adaptive Security Profiler

About

- LWASP is a service to analyze and score vulnerable linux images in preparation for cyber security competitions.
- Very versatile and open to modification, so that coaches and mentors can customize it specifically for their teams if they choose to do so
- Tested on Ubuntu 12.04, 14.04 and 16.04, but should work for all debian-based linux distributions
- Uses Bash and Python for the backend, GTK+3 & Javascript with ReactJS and JQuery for the front end

Initialization

1. Move the lwasp/deploy directory onto a blank or modified image that needs to be scored
2. Open a command prompt (terminal) on the image and run the following commands:
   - `cd /path/to/deploy` (e.g. `cd ~/Desktop/deploy`)
   - `./setup`
3. Check what you want to score and then follow the prompts to install the scoring engine on the image.
4. Advanced users can modify the generated elements.csv file to score advanced elements before finishing installation. See the LWASP Advanced Users Guide for more information.
5. Shut down the image, and distribute it to students. The scoring engine will start on next boot.

Steps for Competitor to Take

1. Once the image is started and they log in, they double click the "Set ID" shortcut on the desktop to set their unique ID. You will receive this ID and the image ID you set during initialization in the email. This is so that if you have several duplicate images, you can tell them apart.
2. They try to secure the image, gaining points by what was set in the elements file.
3. The scoring report will refresh every time a file is changed and once every minute. If this is not often enough or this does not seem to be working, they can type 'sudo refresh' into a terminal to reload the score manually

Troubleshooting

- If the scoring engine does not seem to be refreshing automatically, run the command `sudo refresh`
  - If it returns ‘analyze already running’, wait 10 seconds and try again
  - If this persists, run `sudo rm /etc/lwasp/holder`, followed by `sudo refresh` again

Notes

- You can reach me for contact at steffeydev@icloud.com any questions, concerns, etc
- Forensics questions are in the CyberPatriot model; only checks the text after “ANSWER: “ (can support multiple answers.They try to secure the image, gaining points by what was set in the elements file.
- Remember that some updates are installed on reboot, so some services that you check to score for updating may already be updated when the students boot up the image.