Scripting for Security Part 1

Adrianna Holden-Gouveia
Website: `https://aholdengouveia.name`
: aholdengouveia
: aholdengouveia
: aholdengouveia

Complete the following problems

Please include the script, a screenshot showing it works as intended, cite all sources you used, and give a short explanation of how the script works works and why.

A lot of these would make sense as a cron job, make sure you set up a cron job for at least the snapshot, but feel free to use cron jobs for the rest as well.

1. Write a Script to detect ip addresses trying to gain access, examples of things to pay attention to include all use between midnight and 6, all logins for a specific user, anything else you consider behavior that should send up a red flag. Make sure to include in your assignment what you consider a "red flag" and why

2. Write script to detect changes to a specific directory. Such as changes to /var/log or /etc/ think about using a diff here, or a hash.

3. Monitor hidden files, root executables, and see if changes are made, who made them, and when they were changed

Deliverables

1. Well commented and tested scripts including a link to your GitHub where you've uploaded them.

2. You should have 1 document for your CentOS machine and 1 for your other server.

3. Documentation for scripts should include any changes or updates to the system needed for these scripts to run.

4. Include any assumptions made with justifications, such as: what is considered concerning behavior? which directories are the most concerning if changes are made to them and why?

5. A small paragraph or two explaining if there anything else you think you should have a script and/or cron job for relating to security? why or why not? Must include AT LEAST 3 sources