

Scripting for Server Security Part 2

Adrianna Holden-Gouveia

Website: <https://aholdengouveia.name>

in: aholdengouveia

🔗: aholdengouveia

Complete the following problems

Scripting

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.

1. Take a snapshot of users every other hour (Use a cron job for this) to see if there is any suspicious adding/removing of users
2. Write a script to backup your most important information and your logs. Make sure to note what you consider "your most important information" and why you've decided on that. You should have your script save to a directory you make specifically for backups. You'll need to compress your files in some way.

Documentation

1. Write a document that will show how to control what daemons run on boot and how to change that. assume your audience is technically inclined, but not an expert.
2. Write a one page (or less) document on how to do boot into emergency mode on each server. Include 1 paragraph executive summary on why you might want to.

3. Set up a cron job to run your backup script at specific intervals (daily, weekly, and/or monthly). Document both how you set up the cron job, and make notes on why you've chosen the frequency you have. Frequency of backup MUST include a source on why that timing is a good practice.

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. A short document explaining how to set up a cron job, why they are used, and any sources you used for setting them up. Make sure to include a simple sample for someone to follow
5. Document for the boot system and emergency boot should be focused on how to do each of those things. Audience is someone technically inclined but not an expert. Use screenshots as well as descriptions to guide someone through how to control the daemons and emergency boot.
6. All Sources used should be noted at the end of each document.