

Scripting for Server Security Part 1

Adrianna Holden-Gouveia

Website: <https://aholdengouveia.name>

in: aholdengouveia

Q: aholdengouveia

Complete the following problems

List of AI that can be used for this lab: ChatGPT, Gemini by Google, ClaudeAI by Anthropic, Perplexity, or Microsoft Copilot.

Pick an AI from the list above and complete the following

1. Ask it to make you a script for cybersecurity on your server. What was the prompt you gave it? What changes did you have to make to the script for it to work? What changes did you have to make to the prompt? How many tries did it take to get something that worked? Describe the whole conversation with the AI including all modifications and your testing on the servers.
2. Have the AI add in comments and explanation for the script. Go through each line, look up what it does and compare to what AI said, give a line by line comparison of what you found in your research with links, and what the AI said.
3. Test the script on each server, document how to get the script onto the server, how to run the script, what results should look like. Include screenshots of the script running successfully and any output files.

Pick a different AI from the list above and complete the following

1. Ask it to make you a script for cybersecurity on your server. What was the prompt you gave it? What changes did you have to make to the script for it to work? What changes did you have to make to the prompt? How many tries did it take to get something that worked? Describe the whole conversation with the AI including all modifications and your testing on the servers.
2. Have the AI add in comments and explanation for the script. Go through each line, look up what it does and compare to what AI said, give a line by line comparison of what you found in your research with links, and what the AI said.
3. Test the script on each server, document how to get the script onto the server, how to run the script, what results should look like. Include screenshots of the script running successfully and any output files.

Deliverables

1. Well commented and tested scripts including a link to your GitHub where you've uploaded them, make sure to clearly note what's been done by AI and not you.
2. You should have at least 1 document for your CentOS machine and 1 for your other server. Make sure to clearly label which AI was used for each part.
3. Documentation for scripts should include any changes or updates to the system needed for these scripts to run.
4. Answers to all of the above questions about the AIs used, prompts used, changes, and anything else you needed to answer. Make sure to include answers for BOTH of the AIs used and everything tested on BOTH servers.
5. A small paragraph or two explaining if there is 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