Server Hardening

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

This lab includes a script that was written by me using an AI. Scripts written by AI can be of varying quality, and it's likely you'll get slop and need to fix it. This script is slop on purpose and needs to be fixed. Be wary of the comments by previous developers (me!), you never know who you can trust, here be dragons!

The script is attached to this lab, it's called "BadServerHealthCheck", there is a bash script version and a Python version. You make pick which one you want to fix. There are some hints in the comments for things to fix. Not everything that should be fixed is hinted at, some things that need fixing are included and hidden for extra coding chaos. Let the games begin.

1. Download and install Lynis (https://cisofy.com/lynis/) on both your servers and run it.

2. Create a short report on the findings (one report for each server) and what you'll do to improve your server setup.

3. Fix the given script to monitor the health of your server using the commands from the PowerPoints on Security, DFIR and Backups as your base. Think about what info you care about, and how to make it easier for you to read or upload to your dashboard. Data is only good if you're using it for something.

4. When fixing/debugging/refactoring the script, make sure you also add comments for what each thing actually does.

Deliverables

Scripts with no documentation and no commentary will not be accepted.

Audience is a new intern at the company who's first set of jobs is to check the health of all our report servers here at Acme Corp

1. Your Lynis reports, including any changes you made to each server and why you made those changes.
2. Health Monitoring Document(s)
   (a) Documentation for this should include a short text file explaining what you choose to change on your health monitor and why.
   (b) Location for where the health report is saved and instructions for how to run your script remotely.
   (c) Make sure to include information about what you picked/fixed, why you picked those commands and how they are used.
   (d) Answer the following: Are they different for each server? the same for both? Are the running instructions any different?