CCDC Week 4 Homework

Linux Week

SadServers

Link: https://sadservers.com/scenarios

Finish up any of the SadServers you did not complete during the lab. **Screenshot** proof of completion **and documentation** of how you completed each level. You must complete all 3 challenges below:

Easy #3: Find the secret combination → Must find total number of lines with the string **Alice** and the number next to a single occurrence of **Alice.**

Easy #12: Breaking CSV files → Requires to split up a CSV file into multiple files with a file size restriction.

Medium #23: Fun with Mr Jason → This level is about parsing json data. JQ is a powerful tool that you can use to solve this one.

Troubleshooting Lab

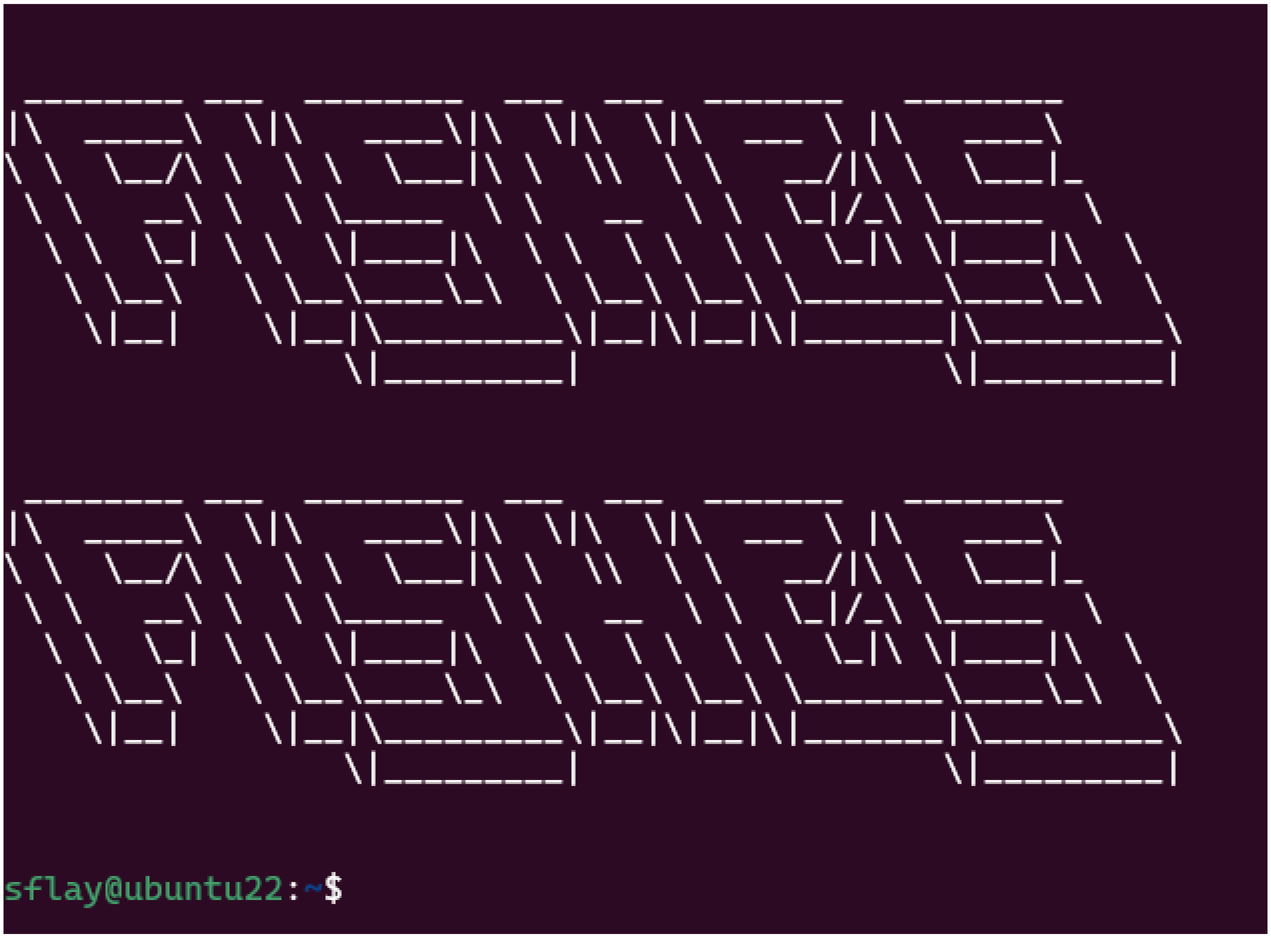
Clone the template `CCDC Linux 2024`. Your CISO has a task for you.
Note: The credentials are `fixer:fixer`. You can use sudo to assume root.

Dear New Employee,

Welcome to Marine Monopolies. I hope you are enjoying your time here. You might've heard about our new fleet of deep-sea submarines. To cut out costs, we've decided to replace the computers in the submarines with the Debian distribution. While the I.T. team was fixing our Windows machines during the CrowdStrike disruption, our Interns replaced existing snapshots with their own… on their last day. Now, we are left with Linux machines with little to no functionality. Please help us fix this please. Attached is a list of issues. Document what you do so we can fix the rest of them.

Respectfully,
Wave Carter

1. Every time **sflay** types out a command, we get a funny picture of this thing or something similar.



```
 ________ ___  ________  ___  ___  _______   ________
|\  _____\  \|\   ____\|\  \|\  \|\  ___ \ |\   ____\
\ \  \__/\ \  \ \  \___|\ \  \\  \ \   __/|\ \  \___|_
 \ \   __\ \  \ \_____  \ \   __  \ \  \_|/_\ \_____  \
  \ \  \_| \ \  \|____|\  \ \  \ \  \ \  \_|\ \|____|\  \
   \ \__\   \ \__\____\_\  \ \__\ \__\ \_______\____\_\  \
    \|__|    \|__|\_________\|__|\|__|\|_______|\_________\
                 \|_________|                  \|_________|


 ________ ___  ________  ___  ___  _______   ________
|\  _____\  \|\   ____\|\  \|\  \|\  ___ \ |\   ____\
\ \  \__/\ \  \ \  \___|\ \  \\  \ \   __/|\ \  \___|_
 \ \   __\ \  \ \_____  \ \   __  \ \  \_|/_\ \_____  \
  \ \  \_| \ \  \|____|\  \ \  \ \  \ \  \_|\ \|____|\  \
   \ \__\   \ \__\____\_\  \ \__\ \__\ \_______\____\_\  \
    \|__|    \|__|\_________\|__|\|__|\|_______|\_________\
                 \|_________|                  \|_________|


sflay@ubuntu22:~$
```

While it was funny, our boss did not find it humorous. Please get rid of this as quickly as possible.

2. We can't hit the Internet from this server. How are we supposed to manage our submarines without Internet? Please fix this. Oh, Jangles tried to fix this one earlier. Multiple things might now be broken.
3. Even before this server lost Internet, we could not download or update anything. Can you fix this?
4. Those pesky interns are trying to spread misinformation about the company. They did something and now a message plays every so often. Please figure out what is causing it and delete the program.
5. Something is wrong with logging in. I didn't notice it at first, but Sue started questioning me on why I logged in 5 times on different servers. Turns out everyone was using my account. Nobody knows my password, so something else is wrong. I did notice that logging in was easier. Even though I always type the wrong password, I've had a 100% login success rate on all authentications.
6. We want to set up some firewalls using iptables, but the command doesn't seem to work. Can you fix that?
7. We are afraid that the interns may have left some users on the machines. Can you do a user audit? The only users should be **sflay**, **jjangles**, **jchen**, and **wcarter**. Also, make sure only **wcarter** and **sflay** (along with yourself) have admin permissions.

Deliverables

1. A screenshot and documentation showing completion of **all 3** SadServer challenges provided
2. Documentation of how you fixed each issue in the provided VM.
   a. Your credentials are `fixer:fixer`
   b. Include:
      i. Steps on how to remediate the issue
      ii. Screenshots of what you did
   c. Make sure to do your due diligence and test your fixes. There may be multiple things broken that allow a problem to exist after fixing one thing.