SSH Configuration

Objectives

In this assignment, you are required to configure and secure the SSH service on a Linux system. Specifically, you must implement the following tasks:

Assignment Requirements

1. **Disable SSH access for the root user**
    - Modify the SSH configuration to prevent the `root` user from logging in via SSH.
    - Restart the SSH service to apply the changes.
2. **Allow a user to use SFTP but deny SSH shell access**
    - Create a new user (e.g., `sftpuser`) who can access the server using SFTP.
    - Restrict this user from accessing an interactive SSH shell.
    - Use a chroot jail to limit access to a specific directory.

3. **Configure SSH Key-Based Authentication**
    - Set up SSH key authentication for a user account (e.g., `studentuser`).
    - Ensure that the user can log in without using a password.
    - Disable password-based SSH login to enhance security.

Submission Instructions

- Submit a short report (PDF) that clearly documents each step you performed.
- Include screenshots of:
    - Configuration files
    - SSH/SFTP test results
    - System status checks (e.g., login attempts, service status)
- Demonstrate and explain the expected results of each configuration.

References

- How To Enable SFTP Without Shell Access on CentOS 7
- How To Set Up SSH Keys on CentOS 7