

1. Log on to the system using the user `ide` and password `ide`.
2. Copy the file `/etc/ca-certificates.conf` to the home directory of the user. The user `ide` must own the copied file.
3. Open up the copy in a text editor and add the following line at the very bottom  
`### COPY OF THE ORIGINAL FILE ###`
4. Find the configuration file for the ssh server and create a backup in the same folder as the file you found. The name of the backup must be the original name plus the extension `.bak`.
5. Open up the original file in a text editor and change the port number to 1022. You must not change ownership of the file.
6. Restart the service `sshd`.
7. Create a bash script called `script1` in the home directory of user `ide`. This script should verify that the first command line argument is a name of an existing directory. If it is not, the script should exit with an error message. Otherwise, it should start the command `"tar -czf /tmp/bak.tgz X"`, where `X` is that directory.
8. Run the script `script1` as a background task, giving `"/usr"` as an argument. After the script is done, make sure it worked!
9. Run the command `ls -la /etc` and store the output in a file `list1.txt` in the home directory of the user `ide`.
10. Create a new user `hos` with password `hos`.
11. In the home directory of the user `hos`, create a file named `fil_1.txt` owned by user `hos`.
12. Rename the `hello world` file in your home directory to `hello1`
13. Create a folder `bin` in your home directory.
14. Remove folder `/tmp/ide` and all it's contents.
15. Create a file (in your home directory) that contains a list of all filenames in the folder `/bin` that start with a `n` or `b`. The file you create should be named `commands_nb.lst`.