Network Security Challenge 04 - Hard

After learning from his mistakes from week 1, Nolan decided to improve his password protected secret store. He created the “Protected Archive for Information and Binary Objects” (PAInBO) to store his secrets. PAInBO now stores secure salted hashes instead of hardcoding the password in the script. To increase security, each account uses multiple passwords that are separately hashed.
The function used to hash the passwords is the following:

```
def calc_hashes(passwords: list[str], username: str) -> list[bytes]:
    return [
        scrypt(password.encode(), salt=username.encode(), n=16384, r=4, p=1)
        for password in passwords
    ]
```

ℹ Exercise 4–2 is hosted at netsec.net.in.tum.de at port 20204.
Please do not try to brute-force a hash in your submitted script.
The scoreboard allows you to upload zip files as your solution. The zip file should contain python script called `solve.py` and other additional files used by the script if necessary.
We recommend connecting to the server using `netcat (man nc)` first.
It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.