1

Skipped. . .

2

With each of the users we know of:

- wizard — ME7WS9H9UXV9DND4

- goblin — 34U97VEYPNODNGZS

- giant — QVN4ZXKH38PGDGS2

- archer — FKGXJP0OCE1LKT3D

we have attempted to login using their credentials.
For all of the users we have got something like:

```
1  > hw4_client.exe
2  Enter username: goblin
3  Enter password: 34U97VEYPNODNGZS
4  Welcome goblin
5
6  What would you like to do?
7  [1] ECHO - ping the server with a custom message, receive the same.
8  [2] TIME - Get local time from server point of view.
9  [3] 2020 - Get a a new year greeting.
10 [4] USER - Show details of registered users.
11 [5] DMSG - Download message from the server.
```

Accept for the archer were we got:

```
1  > hw4_client.exe
2  Enter username: archer
3  Enter password: FKGXJP0OCE1LKT3D
4  Welcome archer (Admin)
5
6  What would you like to do?
7  [1] ECHO - ping the server with a custom message, receive the same.
8  [2] TIME - Get local time from server point of view.
9  [3] 2020 - Get a a new year greeting.
10 [4] USER - Show details of registered users.
11 [5] DMSG - Download message from the server.
12 [6] PEEK - peek into the system.
13 [7] LOAD - Load the content of the last peeked file.
```

Note that not only does the welcome message mention that this user is an admin
- but there are also additional options offered to him. This meant that this user
must have elevated permissions.
The users.py script connects to 'archer' and prints the list of users.

Reverse Engineering - Homework 4

Yosef Goren & Tomer Bitan

July 3, 2023