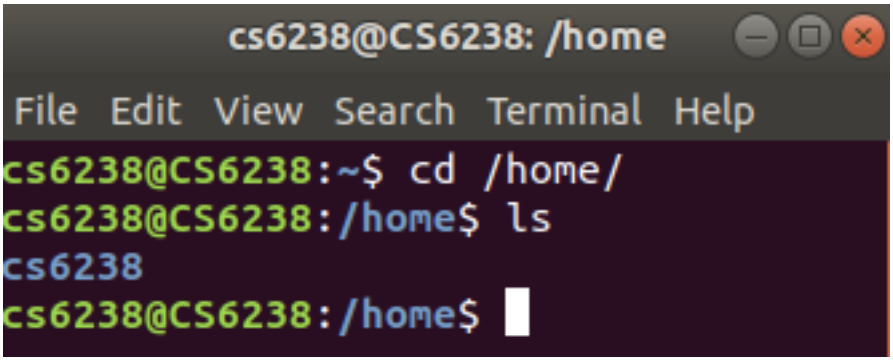
Project II - Password Hardening with 2FA

dvenkatesh7@gatech.edu

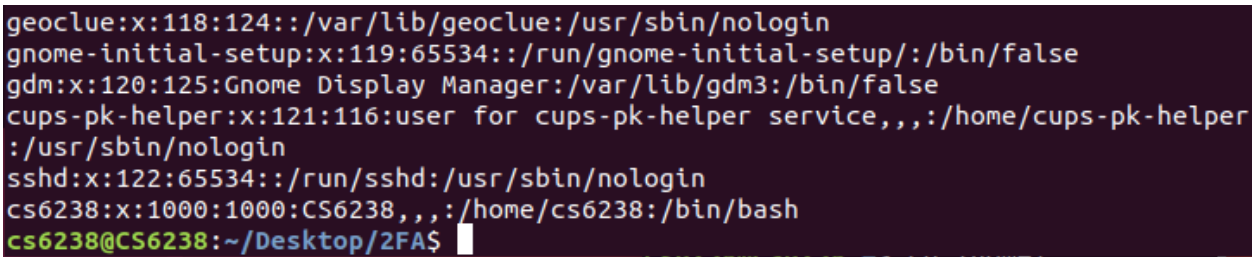
Task1: Implementing 2FA

1. **TEST CASE 1**

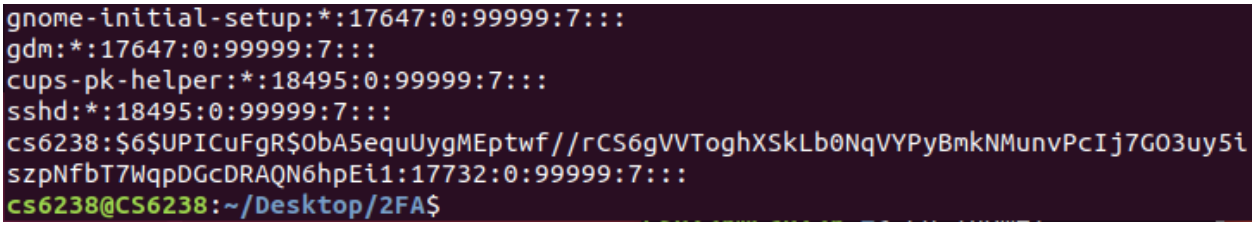
Home folder:



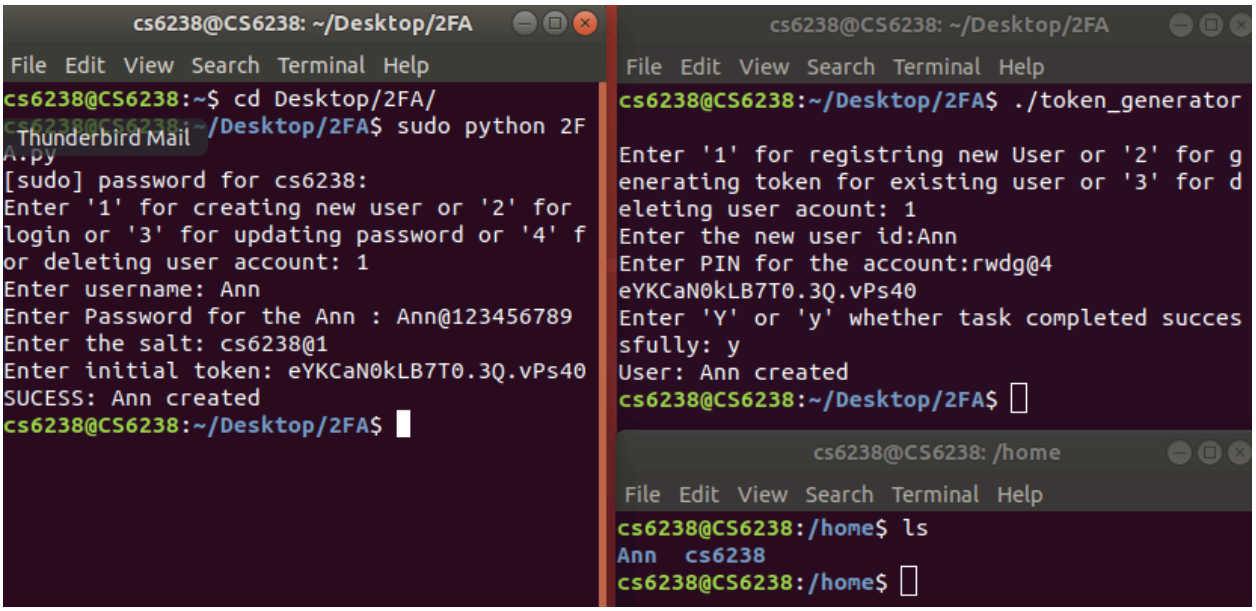
Contents of /etc/passwd:



Contents of /etc/shadow:



2. TEST CASE 2



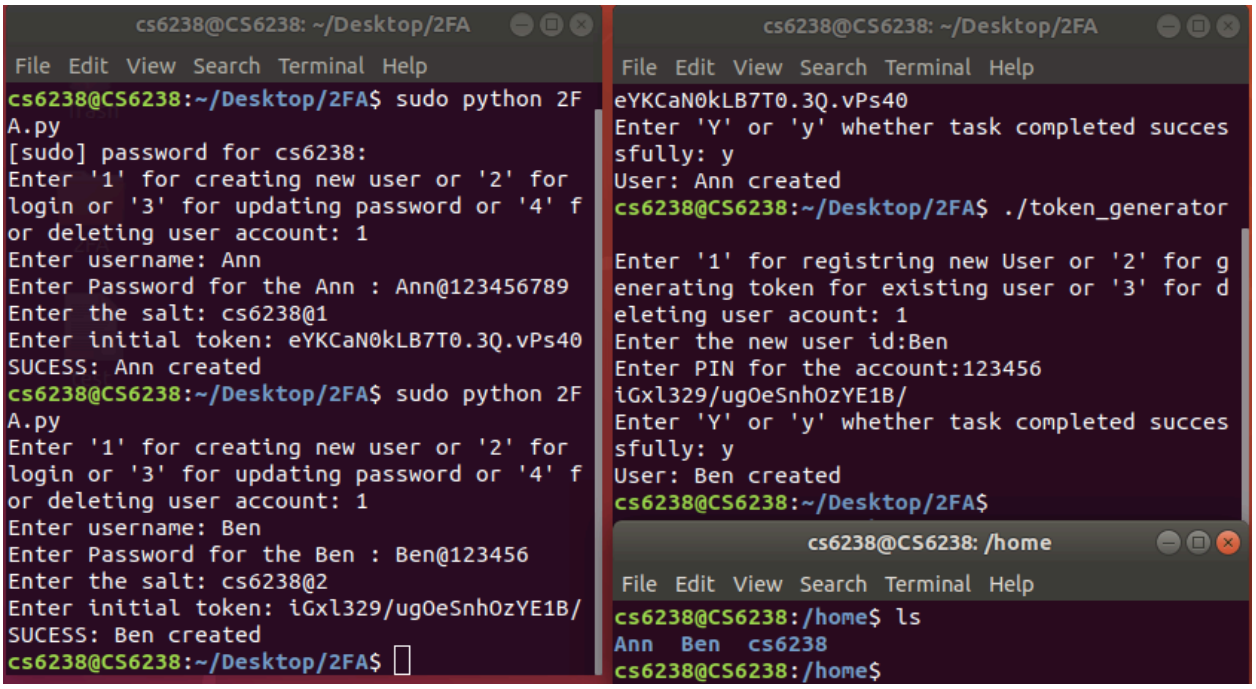
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5i
szpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$cs6238@1$arZo9utD.AIcqxgoKyVukT5ecxaTbZ9mxgZBRTVRbL9ucQp7dH0FHu928fVOCuZ5
94w.CcPDYDVhVqBX1OcfA/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

3. TEST CASE 3



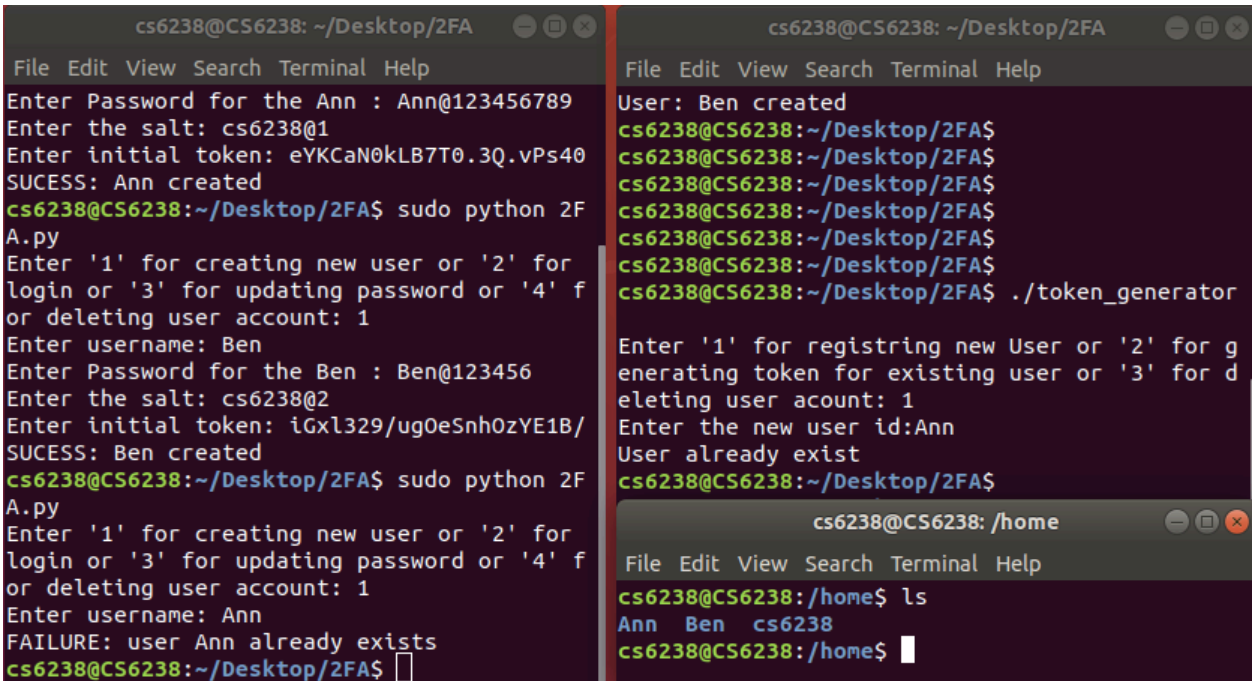
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5i
szpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$cs6238@1$arZo9utD.AIcqxgoKyVukT5ecxaTbZ9mxgZBRTVRbL9ucQp7dH0FHu928fVOCuZ5
94w.CcPDYDVhVqBX1OcfA/:17710:0:99999:7:::
Ben:$6$cs6238@2$iJHifMtbMwS2EWH60XXnkS0ffpTf6YEzZV7whfMniZDsBuAsG7CG7ajmtfZcJ1v8
RZmDwCpDj9YFCvAmJQ3on/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

4. TEST CASE 4



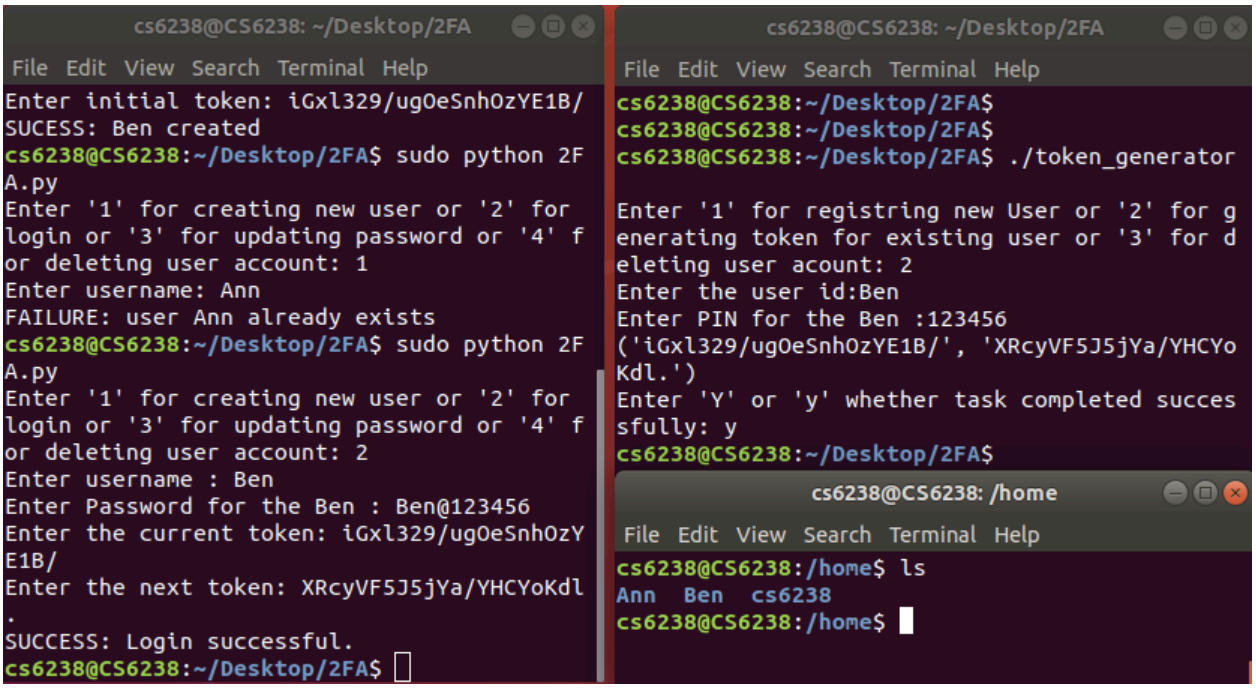
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5iszpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$cs6238@1$arZo9utD.AIcqxgoKyVukT5ecxaTbZ9mxgZBRTVRbL9ucQp7dH0FHu928fVOCuZ594w.CcPDYDVhVqBX1OcfA/:17710:0:99999:7:::
Ben:$6$cs6238@2$iJHifMtbMwS2EWH60XXnkS0ffpTf6YEzZV7whfMniZDsBuAsG7CG7ajmtfZcJ1v8RZmDwCpDj9YFCvAmJQ3on/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

5. TEST CASE 5



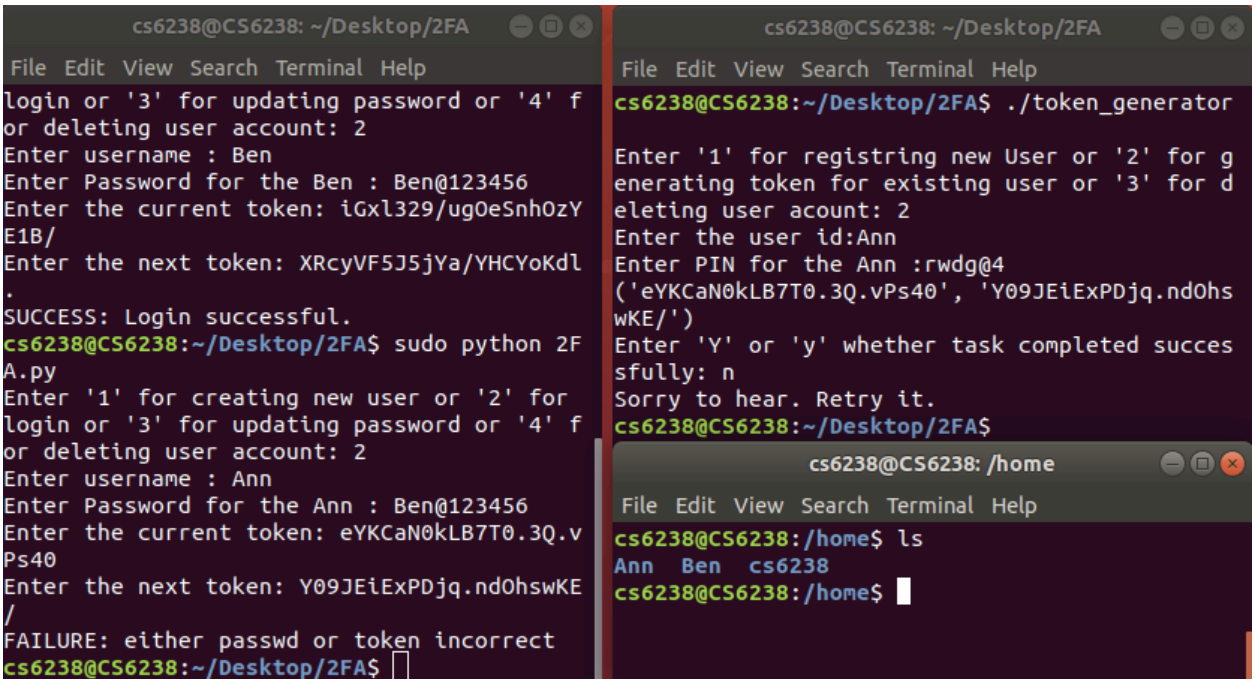
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5i
szpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$cs6238@1$arZo9utD.AIcqxgoKyVukT5ecxaTbZ9mxgZBRTVRbL9ucQp7dH0FHu928fVOCuZ5
94w.CcPDYDVhVqBX1OcfA/:17710:0:99999:7:::
Ben:$6$cs6238@2$yCREPY1gejXW20tH0UMthqERb8kkQ3xcnDWVWQZyAfojqOjd/0hzQ5gv.FuNBssp
zWsQaGPCDZsg845cuxIK0/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

6. TEST CASE 6



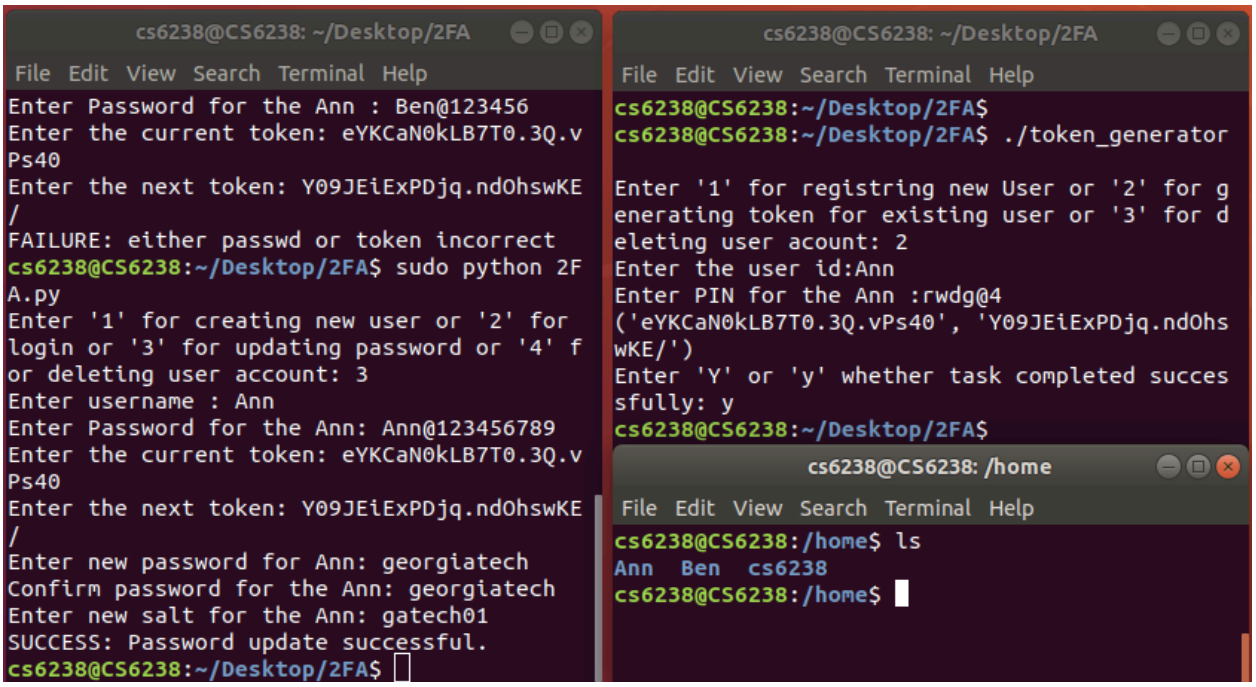
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5i
szpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$cs6238@1$arZo9utD.AIcqxgoKyVukT5ecxaTbZ9mxgZBRTVRbL9ucQp7dH0FHu928fVOCuZ5
94w.CcPDYDVhVqBX1OcfA/:17710:0:99999:7:::
Ben:$6$cs6238@2$yCREPY1gejXW20tH0UMthqERb8kkQ3xcnDWVWQZyAfojqOjd/0hzQ5gv.FuNBssp
zWsQaGPCDZsg845cuxIK0/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

7. TEST CASE 7



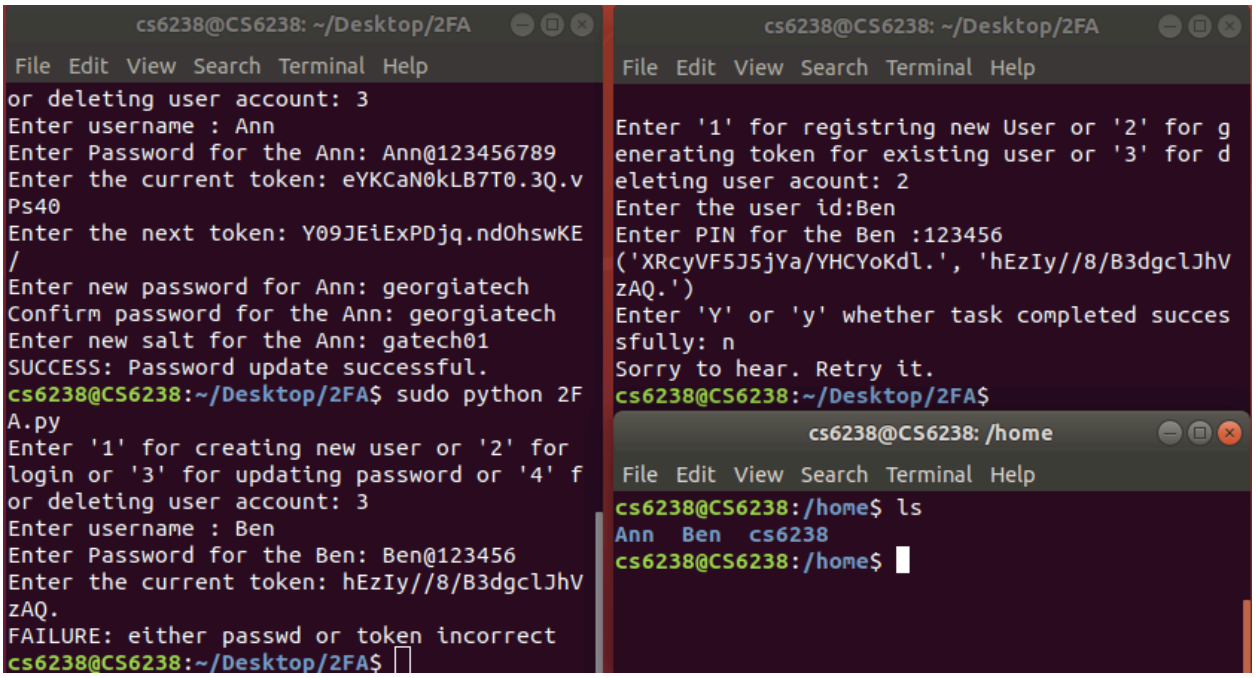
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5iszpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$gatech01$wI1ZfbwsgLiZseyUcKA6.ELzUmB/ZvV3EAFjmBDw6qsTugJAMOMcMwl5MLYsGxoaz4RP5zt8EbwK/jqMbVoX20:17710:0:99999:7:::
Ben:$6$cs6238@2$yCREPY1gejXW20tH0UMthqERb8kkQ3xcnDWVWQZyAfojqOjd/0hzQ5gv.FuNBsspzWsQaGPCDZsg845cuxIK0/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

8. TEST CASE 8



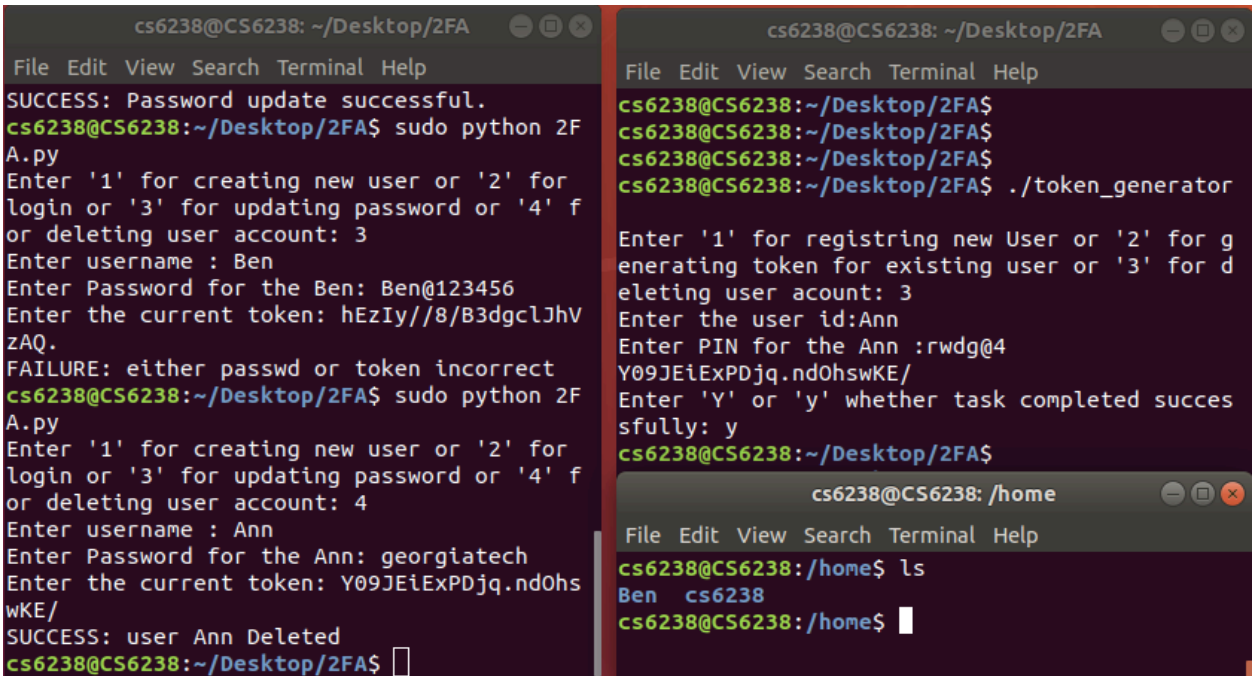
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ann:x:1001:1001:,,,:/home/Ann:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5iszpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ann:$6$gatech01$wI1ZfbwsgLiZseyUcKA6.ELzUmB/ZvV3EAFjmBDw6qsTugJAMOMcMwl5MLYsGxoaz4RP5zt8EbwK/jqMbVoX20:17710:0:99999:7:::
Ben:$6$cs6238@2$yCREPY1gejXW20tH0UMthqERb8kkQ3xcnDWVWQZyAfojqOjd/0hzQ5gv.FuNBsspzWsQaGPCDZsg845cuxIK0/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

9. TEST CASE 9



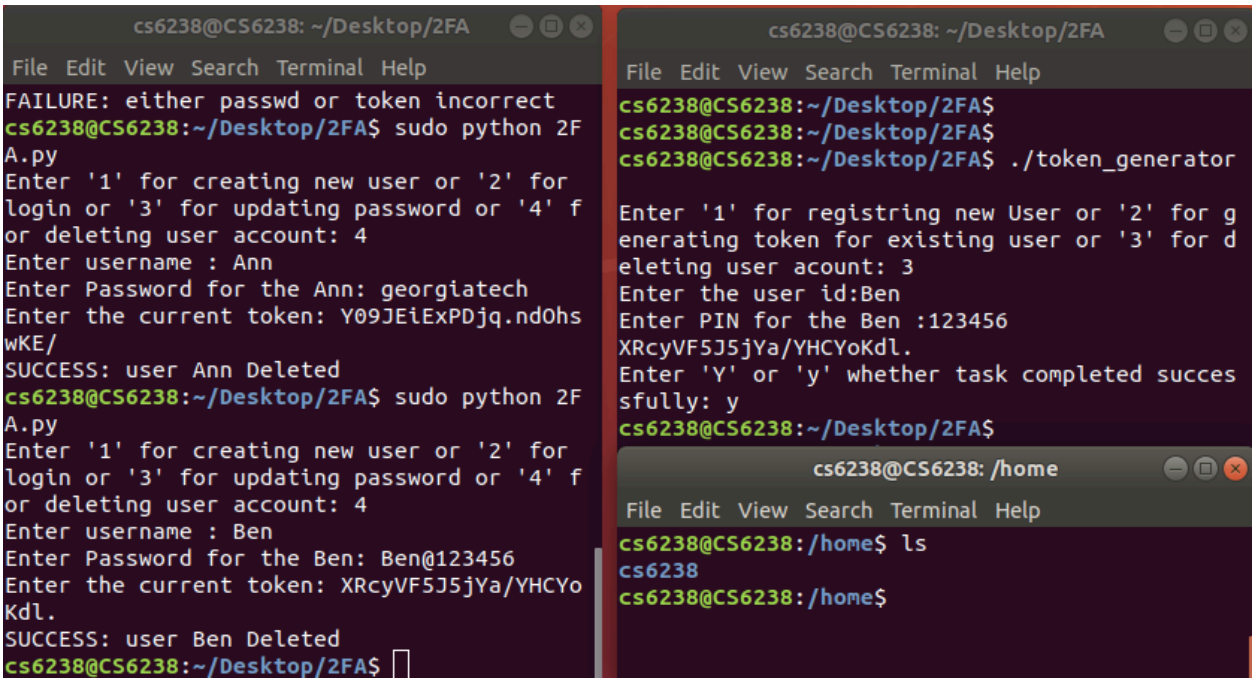
Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
Ben:x:1002:1002:,,,:/home/Ben:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5i
szpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
Ben:$6$cs6238@2$yCREPY1gejXW20tH0UMthqERb8kkQ3xcnDWVWQZyAfojqOjd/0hzQ5gv.FuNBssp
zWsQaGPCDZsg845cuxIK0/:17710:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

10. TEST CASE 10



Contents of /etc/passwd:

```
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
cups-pk-helper:x:121:116:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cs6238:x:1000:1000:CS6238,,,:/home/cs6238:/bin/bash
cs6238@CS6238:~/Desktop/2FA$
```

Contents of /etc/shadow:

```
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
cups-pk-helper:*:18495:0:99999:7:::
sshd:*:18495:0:99999:7:::
cs6238:$6$UPICuFgR$ObA5equUygMEptwf//rCS6gVVToghXSkLb0NqVYPyBmkNMunvPcIj7GO3uy5iszpNfbT7WqpDGcDRAQN6hpEi1:17732:0:99999:7:::
cs6238@CS6238:~/Desktop/2FA$
```

Task2: Security Analysis of 2FA

1. ***2 advantages of the 2FA method implemented above*:**

   a. 2FA adds an additional level of security making it difficult for the attacker to login to the system. This method uses a token generator is used as the second factor. The tokens that it gives is entered into the 2FA method to perform the authentication.
   b. The passwords are not stored directly in the /etc/shadow file. Instead, a salt value is added and a hash of it is stored. Even if attacker gets hold of this file, it will be difficult to crack the password.
   Concatenating the user password with the tokens obtained from token generator, a hardened password is generated which is in turn hashed and stored. This makes the system secure.

   2 disadvantages of the 2FA method implemented above:

   a. The 2FA introduces an additional step while logging in. If the user doesn't have the token generation device, he might not be able to login to the system.
   b. The other disadvantage is that the token generator will keep producing the same tokens until the 2FA method was successfully completed. So, the attacker can keep using the same tokens until he successfully logs in to the system.

   2 possible attacks on the 2FA method implemented above:

   a. As we mentioned earlier, the token generator will generate same set of tokens until the 2FA method was successfully executed. So, the attacker can get hold of this and keep using it to perform the login.
   b. The attacker can use a keylogger to get hold of the user password. And he can also get the token as discussed in the above point and generate the hardened password and try to login to the system.

2. ***Improvement for the current 2FA scheme:***

   In the current implementation, the user has to generate the tokens and copy paste them manually in the 2FA method. This step is error prone. The user may enter the tokens incorrectly or may swap the current and next token while entering. This will result in lot of false negatives. To avoid this, instead of manually entering the tokens, the token generator can generate the tokens automatically and send it to the 2FA method.

   By doing this the additional step of copy pasting will be eliminated. This will also avoid users entering wrong tokens during the process and also it will adhere to the principle of user acceptability as the user doesn't have to manually enter the tokens.

The other improvement that can be implemented is, the token generator should return a different token every single time irrespective of whether the 2FA method execution was successful or not. Currently, the token generator is returning the same tokens until the 2FA method is successfully completed. This will enable the attacker to keep trying to login with the same token if he gets the token. But by returning a different token every time, it becomes very difficult for the attacker to guess the token.

3. ***Implement 2FA on a server client setting:***

When the user(client) is trying to login, he will send a request to the server which has the token generator to provide the required tokens. The server based on the input will reply to the client with the requested tokens. These values are inputted to the login process at the client to perform the login process.

Since here the server and client are accessing sensitive information, the payload should be end-end encrypted. The exchange of tokens between client and server can be secured with the SSL/TSL protocols.

Additionally, a load balancer can be used to equally distribute the traffic across servers that can fulfil the client request.