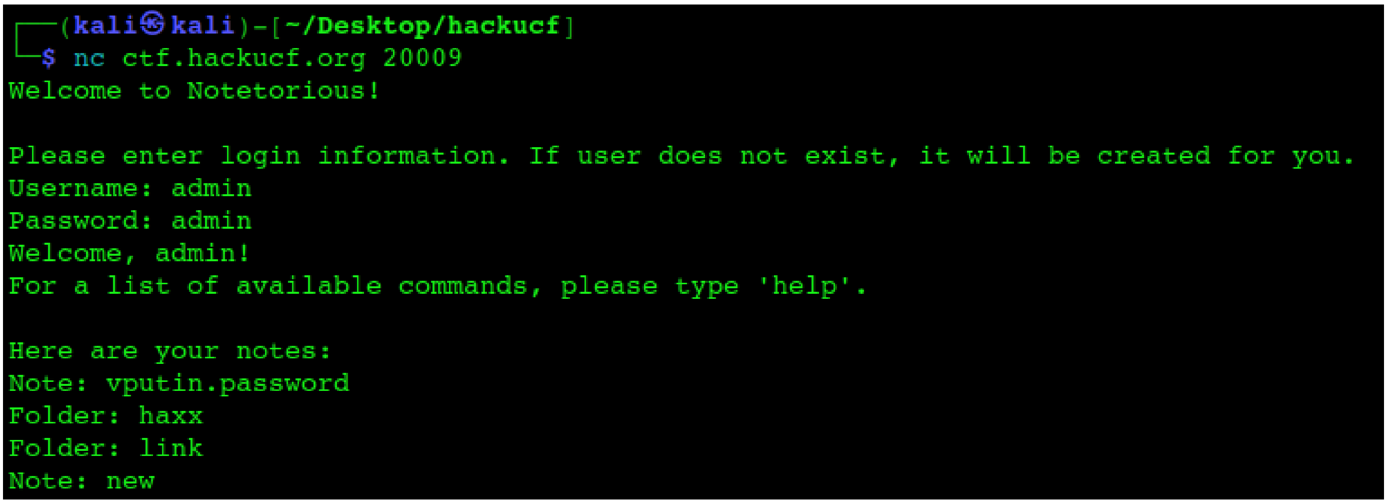
Notetorious

Challenge

> Agent,
> We have determined that Vladimir Putin uses an online note taking service called Notetorious.
> His username on this service is vputin. Your objective is to exfiltrate his secret notes.

We are only given a port to connect to: `nc ctf.hackucf.org 20009`

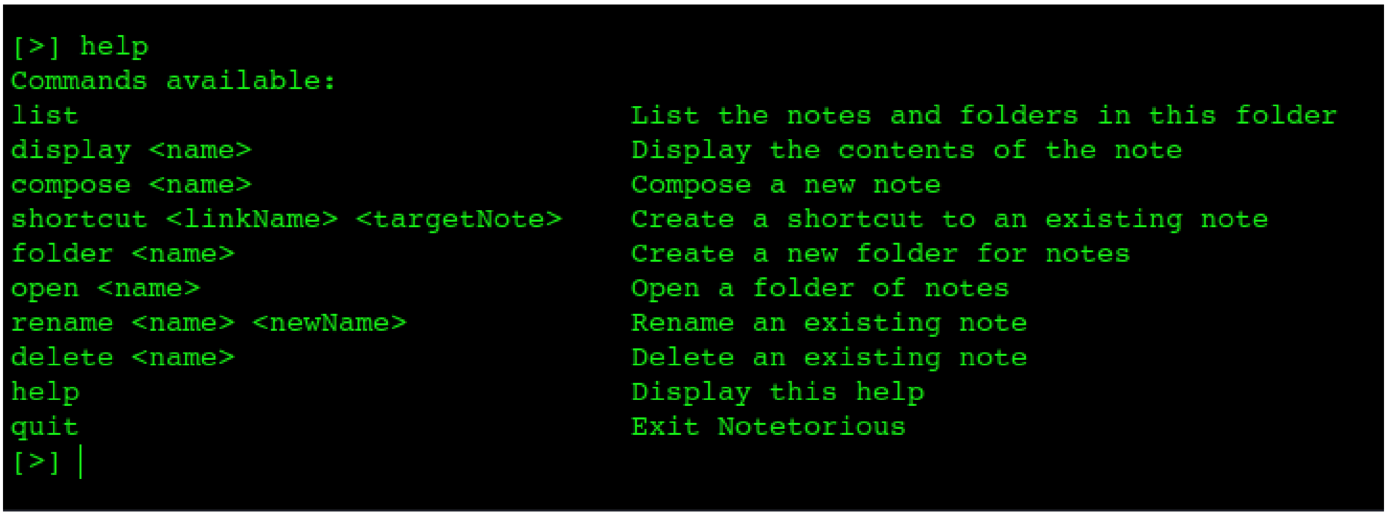


```
┌──(kali㉿kali)-[~/Desktop/hackucf]
└─$ nc ctf.hackucf.org 20009
Welcome to Notetorious!

Please enter login information. If user does not exist, it will be created for you.
Username: admin
Password: admin
Welcome, admin!
For a list of available commands, please type 'help'.

Here are your notes:
Note: vputin.password
Folder: haxx
Folder: link
Note: new
```

After connecting, I saw a message 'If user does not exist, it will be created for you.' so I attempted to log in as user admin with password admin.

This gave me access to the system.

It appeared that I had two folders already and a password file.



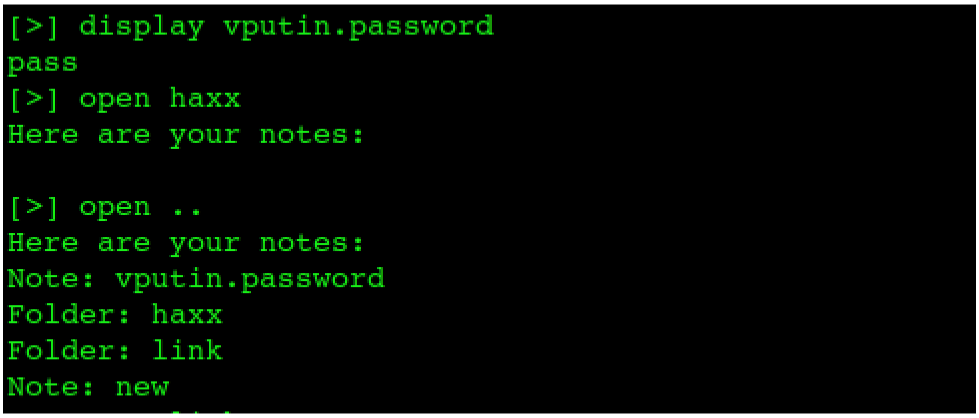
```
[>] help
Commands available:
list                                List the notes and folders in this folder
display <name>                      Display the contents of the note
compose <name>                      Compose a new note
shortcut <linkName> <targetNote>    Create a shortcut to an existing note
folder <name>                       Create a new folder for notes
open <name>                         Open a folder of notes
rename <name> <newName>             Rename an existing note
delete <name>                       Delete an existing note
help                                Display this help
quit                                Exit Notetorious
[>] |
```

Running the help command showed which commands were available.

A few commands were of note to me,

- list = ls
- display = cat
- open = cd

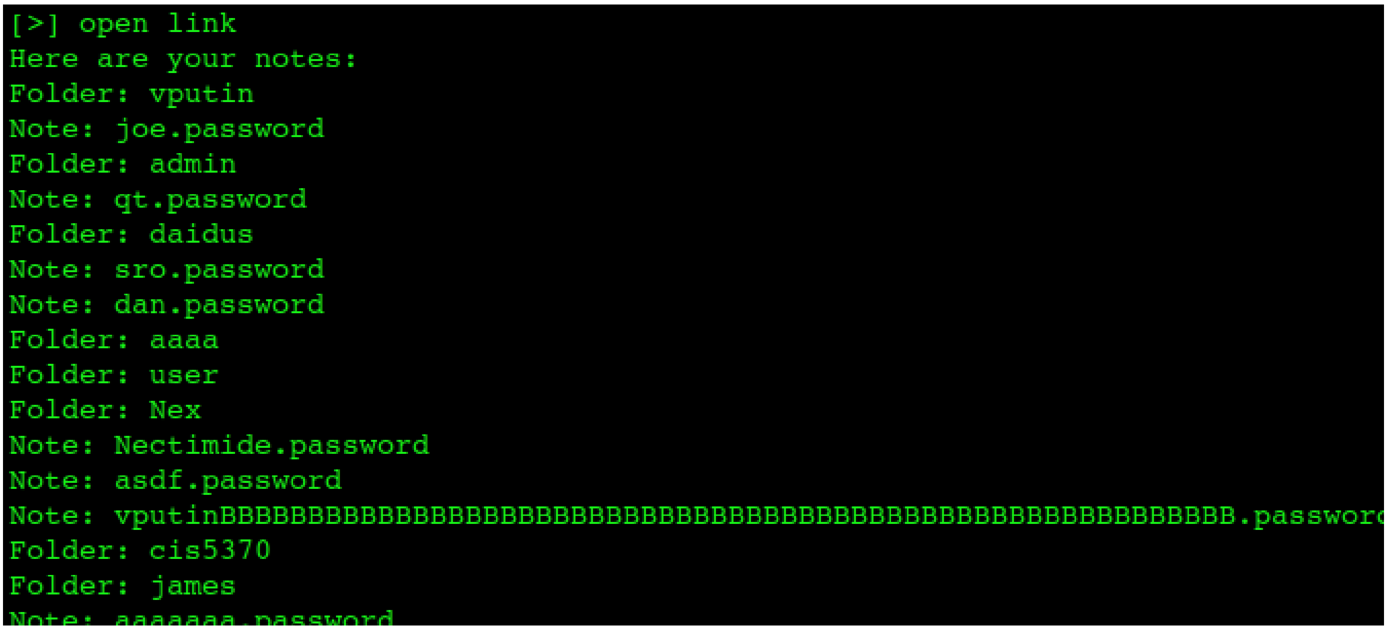
Solution



```
[>] display vputin.password
pass
[>] open haxx
Here are your notes:

[>] open ..
Here are your notes:
Note: vputin.password
Folder: haxx
Folder: link
Note: new
```

I first attempted to open the password file, but found nothing.

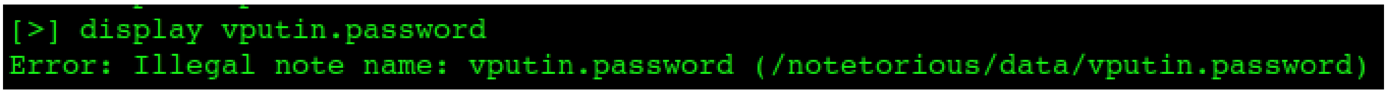
Then I moved to the haxx folder and also found nothing.



```
[>] open link
Here are your notes:
Folder: vputin
Note: joe.password
Folder: admin
Note: qt.password
Folder: daidus
Note: sro.password
Note: dan.password
Folder: aaaa
Folder: user
Folder: Nex
Note: Nectimide.password
Note: asdf.password
Note: vputinBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB.passwor
Folder: cis5370
Folder: james
Note: aaaaaaa.password
```

However, when opening the link folder I found many files.

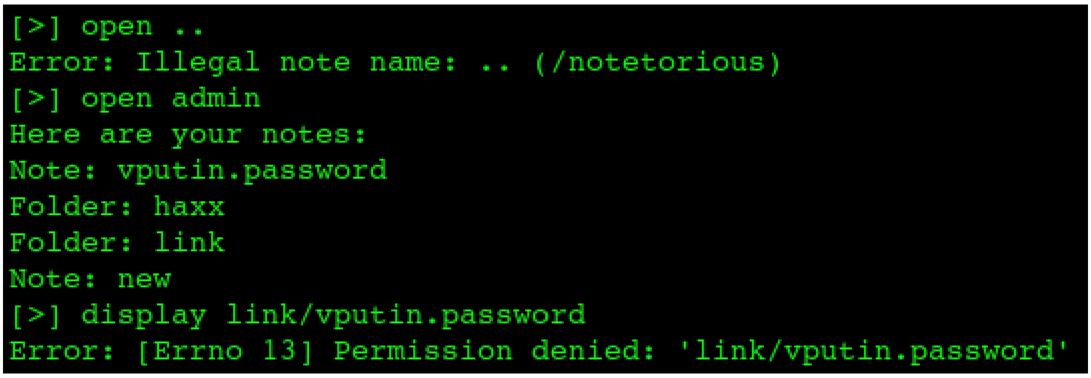
In the link folder, all the users' home directories and passwords were stored.



```
[>] display vputin.password
Error: Illegal note name: vputin.password (/notetorious/data/vputin.password)
```

From the challenge description, I knew that vputin was the user of interest.

I attempted to open the vputin.password file and was given an illegal note name error.

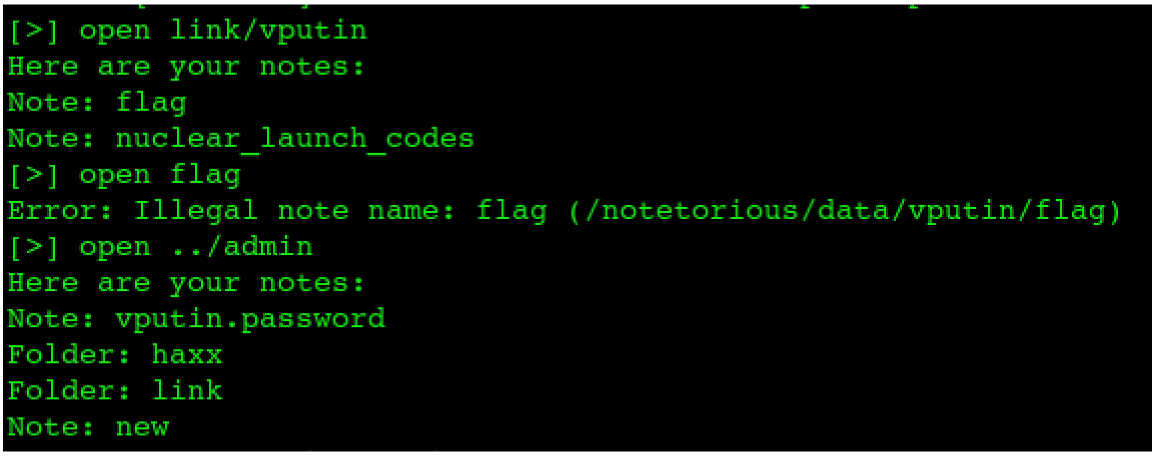


```
[>] open ..
Error: Illegal note name: .. (/notetorious)
[>] open admin
Here are your notes:
Note: vputin.password
Folder: haxx
Folder: link
Note: new
[>] display link/vputin.password
Error: [Errno 13] Permission denied: 'link/vputin.password'
```

So, I then tried to open the file using the link folder.

After navigating back to my home directory I could in fact access the file; however, I got a different error 'permission denied'.

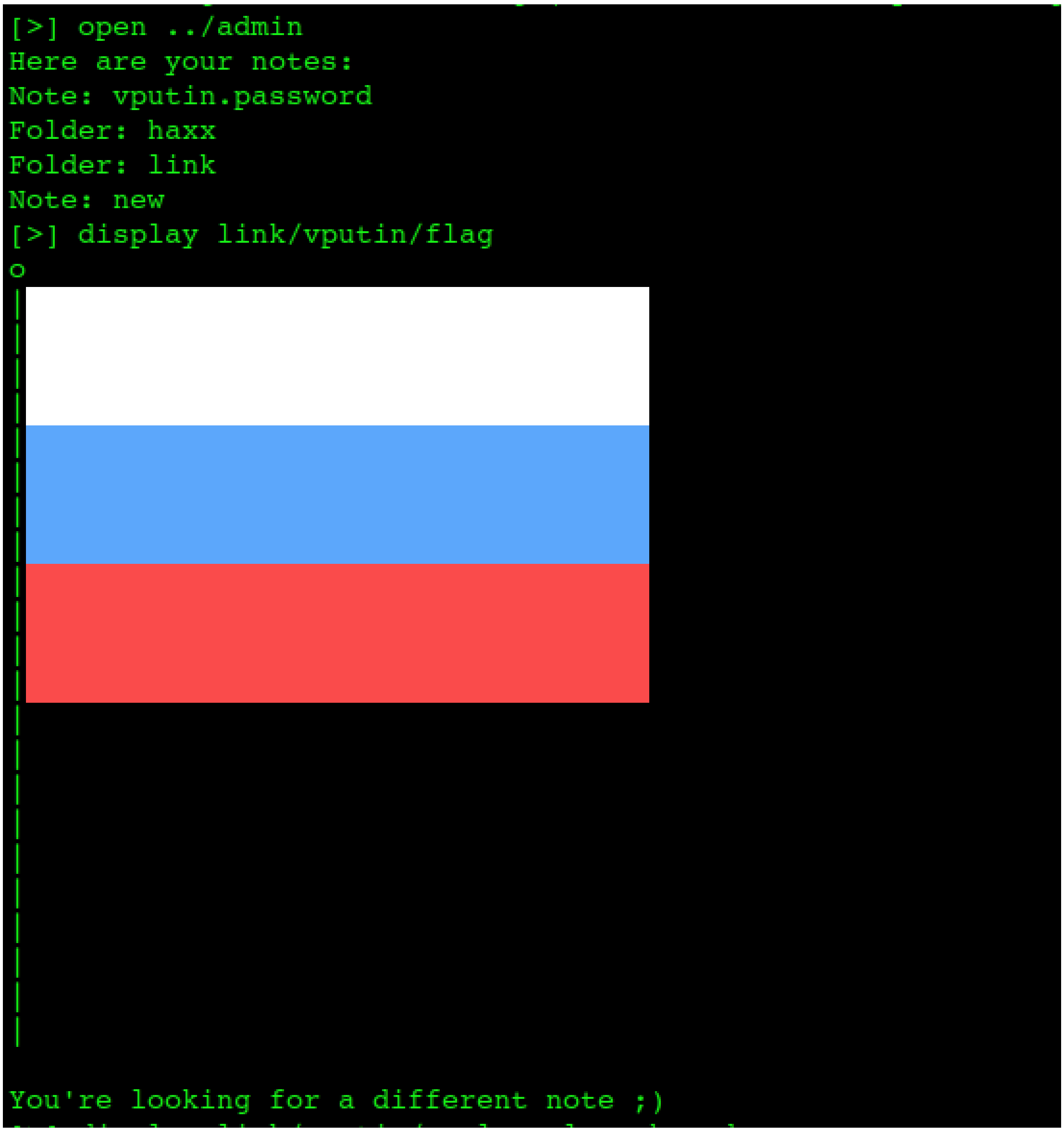
I noticed that each user was allocated a directory, as I used open admin to navigate back to my starting folder.



```
[>] open link/vputin
Here are your notes:
Note: flag
Note: nuclear_launch_codes
[>] open flag
Error: Illegal note name: flag (/notetorious/data/vputin/flag)
[>] open ../admin
Here are your notes:
Note: vputin.password
Folder: haxx
Folder: link
Note: new
```

Knowing this I then tried to locate and open vputin's folder.

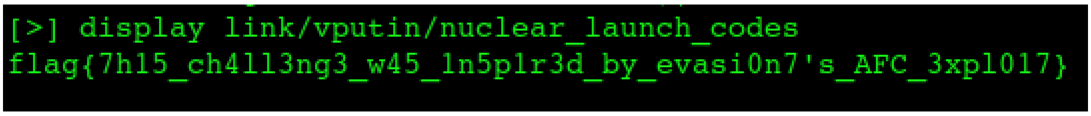
And this worked! However, I was given the same illegal note name error as before.



```
[>] open ../admin
Here are your notes:
Note: vputin.password
Folder: haxx
Folder: link
Note: new
[>] display link/vputin/flag
o
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|

You're looking for a different note ;)
```

I navigated back to my starting folder again and attempted to access vputin's files via the link folder; now I had access!

When opening the flag file, I was given a real flag and not the challenge flag.



```
[>] display link/vputin/nuclear_launch_codes
flag{7h15_ch4ll3ng3_w45_1n5p1r3d_by_evasi0n7's_AFC_3xpl017}
```

Vputin still had another file in his folder.

When opening this file, I found the flag I was looking for.